Journal officiel
de l'Union européenne

FR
Série L

2025/327

5.3.2025

RÈGLEMENT (UE) 2025/327 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 11 février 2025

relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

vu l'avis du Comité des régions ([2]),

statuant conformément à la procédure législative ordinaire ([3]),

considérant ce qui suit:

(1) L'objectif du présent règlement est d'établir l'espace européen des données de santé (EEDS) afin d'améliorer l'accès des personnes physiques à leurs données de santé électroniques à caractère personnel et leur contrôle sur ces données dans le contexte des soins de santé, ainsi que pour mieux atteindre d'autres finalités impliquant l'utilisation de données de santé électroniques dans les secteurs des soins de santé et des soins qui bénéficieraient à la société, telles que la recherche, l'innovation, l'élaboration des politiques, la préparation et la réaction aux menaces sanitaires, y compris la prévention des pandémies à venir et la réponse à y apporter, la sécurité des patients, la médecine personnalisée, les statistiques officielles ou les activités réglementaires. En outre, l'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique et technique uniforme, en particulier pour le développement, la commercialisation et l'utilisation des systèmes de dossiers médicaux électroniques (ci-après dénommés «systèmes de DME») en conformité avec les valeurs de l'Union. L'EEDS sera un élément clé de la création d'une Union de la santé européenne forte et résiliente.

(2) La pandémie de COVID-19 a mis en évidence l'impératif de disposer d'un accès rapide à des données de santé électroniques de qualité à des fins de préparation et de réaction aux menaces sanitaires, ainsi qu'à des fins de prévention, de diagnostic et de traitement et à des fins d'utilisation secondaire de ces données de santé électroniques. Cet accès rapide pourrait potentiellement contribuer, par une surveillance et un suivi efficients de la santé publique, à une gestion plus efficace des pandémies à venir, à une réduction des coûts et à une amélioration de la réaction aux menaces sanitaires et pourrait contribuer en définitive à sauver plus de vies. En 2020, la Commission a adapté d'urgence son système de gestion des données cliniques des patients, établi par la décision d'exécution (UE) 2019/1269 de la Commission ([4]), afin de permettre aux États membres de partager les données de santé électroniques des patients atteints de COVID-19 passant d'un prestataire de soins de santé et d'un État membre à un autre au plus fort de cette pandémie. Toutefois, cette adaptation n'était qu'une solution d'urgence, montrant la nécessité d'une approche structurelle et cohérente à l'échelon des États membres et à l'échelon de l'Union à la fois pour améliorer la disponibilité des données de santé électroniques pour les soins de santé et pour faciliter l'accès aux données de santé électroniques afin d'orienter des réponses politiques efficaces et de contribuer à des normes élevées en matière de santé humaine.

(3) La crise de la COVID-19 a fermement consolidé le travail du réseau «Santé en ligne», un réseau volontaire d'autorités chargées de la santé numérique, en tant que principal pilier pour le développement d'applications de recherche des contacts et d'alerte des contacts pour les appareils mobiles et pour les aspects techniques des certificats COVID

([1]) JO C 486 du 21.12.2022, p. 123.
([2]) JO C 157 du 3.5.2023, p. 64.
([3]) Position du Parlement européen du 24 avril 2024 (non encore parue au Journal officiel) et décision du Conseil du 21 janvier 2025.
([4]) Décision d'exécution (UE) 2019/1269 de la Commission du 26 juillet 2019 modifiant la décision d'exécution 2014/287/UE établissant les critères de mise en place et d'évaluation des réseaux européens de référence et de leurs membres et de facilitation des échanges d'informations et de connaissances liées à la mise en place de ces réseaux et à leur évaluation (JO L 200 du 29.7.2019, p. 35).

numériques de l'UE. Elle a aussi mis en évidence la nécessité de partager des données de santé électroniques faciles à trouver, accessibles, interopérables et réutilisables (les principes «FAIR»), et de garantir que les données de santé électroniques sont aussi ouvertes que possible, tout en respectant le principe de la minimisation des données énoncé dans le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]). Des synergies entre l'EEDS, le nuage européen pour la science ouverte et les infrastructures de recherche européennes devraient être assurées, et des enseignements devraient être tirés des solutions de partage des données mises au point au titre de la plateforme européenne de données sur la COVID-19.

(4) Étant donné le caractère sensible des données de santé électroniques à caractère personnel, le présent règlement vise à fournir des garanties suffisantes, tant au niveau de l'Union qu'au niveau national, afin de garantir un niveau élevé de protection, de sécurité, de confidentialité et d'utilisation éthique des données. Ces garanties sont nécessaires pour renforcer la confiance dans la sécurité de traitement des données de santé électroniques des personnes physiques à des fins d'utilisation primaire et d'utilisation secondaire telles que celles-ci sont définies dans le présent règlement.

(5) Le traitement des données de santé électroniques à caractère personnel est soumis aux dispositions du règlement (UE) 2016/679 et, pour les institutions, organes et organismes de l'Union, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]). Les références aux dispositions du règlement (UE) 2016/679 devraient s'entendre comme des références faites aux dispositions correspondantes du règlement (UE) 2018/1725 pour les institutions, organes et organismes de l'Union, le cas échéant.

(6) De plus en plus de personnes vivant dans l'Union franchissent les frontières nationales pour travailler, étudier, rendre visite à des proches ou pour d'autres raisons. Afin de faciliter l'échange de données de santé, et conformément à la nécessité d'autonomiser les citoyens, ceux-ci devraient pouvoir accéder à leurs données de santé dans un format électronique qui puisse être reconnu et accepté partout dans l'Union. Ces données de santé électroniques à caractère personnel pourraient inclure des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris celles relatives à la fourniture de services de soins de santé, et qui révèlent des informations sur l'état de santé de cette personne physique, des données à caractère personnel relatives aux caractéristiques génétiques innées ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou la santé d'une personne physique et qui résultent, en particulier, d'une analyse d'un échantillon biologique de la personne physique en question, ainsi que des données sur des facteurs déterminants pour la santé, tels que le comportement, les facteurs environnementaux et les influences physiques, les soins médicaux, ainsi que les facteurs sociaux ou éducatifs. Les données de santé électroniques comprennent également les données qui ont été initialement collectées à des fins de recherche, de statistiques, d'évaluation des menaces sanitaires, d'élaboration de politiques ou de réglementations et il devrait être possible de les mettre à disposition conformément aux règles établies dans le présent règlement. Les données de santé électroniques comprennent toutes les catégories de ces données, indépendamment du fait que ces données sont fournies par la personne concernée ou par d'autres personnes physiques ou morales, telles que des professionnels de la santé, ou qu'elles sont traitées en relation avec la santé ou le bien-être d'une personne physique, et devraient également inclure les données déduites et dérivées, telles que les diagnostics, les analyses et les examens médicaux, ainsi que les données observées et enregistrées par des procédés automatisés.

(7) Dans les systèmes de santé, les données de santé électroniques à caractère personnel sont habituellement rassemblées dans des dossiers médicaux électroniques, qui contiennent généralement les antécédents médicaux, les diagnostics et traitements, les médicaments, les allergies et les vaccinations, ainsi que les images de radiologie, les résultats de laboratoire, ainsi que d'autres données médicales d'une personne physique, partagées par les différents acteurs dans le système de santé, tels que les médecins généralistes, hôpitaux, pharmacies ou services de soins. Afin d'autoriser les personnes physiques ou les professionnels de la santé à accéder aux données de santé électroniques, à les partager ou à les modifier, certains États membres ont pris les mesures juridiques et techniques nécessaires et ont mis en place des infrastructures centralisées qui connectent les systèmes de DME utilisés par les prestataires de soins de santé et les personnes physiques. En outre, certains États membres aident les prestataires de soins de santé publics et privés à mettre en place des espaces de données de santé électroniques à caractère personnel afin de permettre l'interopérabilité entre les différents prestataires de soins de santé. Plusieurs États membres soutiennent aussi ou fournissent des services d'accès aux données de santé électroniques pour les patients et les professionnels de la santé, par exemple au moyen de portails destinés aux patients ou aux professionnels de la santé. Ces États membres ont aussi pris des mesures pour garantir que les systèmes de DME ou les applications de bien-être peuvent transmettre les données de santé électroniques au système de DME central, par exemple en prévoyant un système de certification. Tous les États membres n'ont cependant pas mis en place de tels systèmes, et les États membres qui l'ont fait les ont mis en place de manière fragmentée. Afin de faciliter la libre circulation des données de santé électroniques

([5]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

à caractère personnel dans toute l'Union et d'éviter des conséquences négatives pour les patients lorsqu'ils reçoivent des soins de santé dans un contexte transfrontière, une action de l'Union est nécessaire pour améliorer l'accès des personnes physiques à leurs propres données de santé électroniques à caractère personnel et pour leur permettre de partager ces données. À cet égard, il convient de prendre des mesures appropriées au niveau de l'Union et au niveau national afin de réduire la fragmentation, l'hétérogénéité et les divisions, et pour mettre en place un système convivial et intuitif dans tous les États membres. Toute transformation numérique dans le secteur des soins de santé devrait tendre à l'inclusivité et bénéficier aussi aux personnes physiques dont les capacités d'accès aux services numériques et d'utilisation des services numériques sont limitées, y compris les personnes handicapées.

(8) Le règlement (UE) 2016/679 contient des dispositions spécifiques concernant les droits des personnes physiques à l'égard du traitement de leurs données à caractère personnel. L'EEDS s'appuie sur ces droits et complète certains d'entre eux tels qu'ils s'appliquent aux données de santé électroniques à caractère personnel. Ces droits s'appliquent indépendamment de l'État membre dans lequel les données de santé électroniques à caractère personnel sont traitées, du type de prestataire de soins de santé, des sources de ces données ou de l'État membre d'affiliation de la personne physique. Les règles et droits relatifs à l'utilisation primaire des données de santé électroniques à caractère personnel au titre du présent règlement concernent toutes les catégories de ces données, indépendamment de la manière dont elles ont été collectées ou de la personne qui les a fournies, du fondement juridique du traitement au titre du règlement (UE) 2016/679 ou du statut du responsable du traitement en tant qu'organisation publique ou privée. Les droits supplémentaires d'accès et de portabilité concernant les données de santé électroniques à caractère personnel prévus par le présent règlement devraient être sans préjudice des droits d'accès et de portabilité établis par le règlement (UE) 2016/679. Les personnes physiques continuent à jouir de ces droits dans les conditions prévues par ledit règlement.

(9) Tandis que les droits conférés par le règlement (UE) 2016/679 devraient continuer de s'appliquer, le droit d'accès aux données par une personne physique, établi par le règlement (UE) 2016/679, devrait être développé davantage dans le secteur des soins de santé. En vertu dudit règlement, les responsables du traitement ne doivent pas fournir un accès immédiat. Le droit d'accès aux données de santé est encore communément mis en œuvre à de nombreux endroits par la fourniture des données de santé demandées sur support papier ou sous la forme de documents numérisés, ce qui prend du temps pour le responsable du traitement, tel que l'hôpital ou un autre prestataire de soins de santé fournissant l'accès. Cette situation ralentit l'accès des personnes physiques aux données de santé et peut avoir une incidence négative sur celles-ci si elles ont besoin d'un accès immédiat à ces données en raison de situations d'urgence concernant leur état de santé. Il est par conséquent nécessaire de prévoir un moyen plus efficace permettant aux personnes physiques d'accéder à leurs propres données de santé électroniques à caractère personnel. Elles devraient avoir un droit d'accès gratuit et immédiat, tout en respectant le besoin de faisabilité technique, aux catégories prioritaires spécifiques de données de santé électroniques à caractère personnel, telles que leur résumé du dossier de patient, par l'intermédiaire d'un service d'accès aux données de santé électroniques. Ce droit devrait s'appliquer indépendamment de l'État membre dans lequel les données de santé électroniques à caractère personnel sont traitées, du type de prestataire de soins de santé, des sources de ces données ou de l'État membre d'affiliation de la personne physique. La portée de ce droit complémentaire établi en vertu du présent règlement et les conditions de son exercice diffèrent à certains égards du droit d'accès aux données à caractère personnel au titre du règlement (UE) 2016/679, lequel couvre toutes les données à caractère personnel détenues par un responsable du traitement et est exercé à l'encontre d'un responsable du traitement individuel, qui dispose d'un mois maximum pour répondre à une demande. Le droit d'accès aux données électroniques de santé à caractère personnel prévu par le présent règlement devrait être limité aux catégories de données entrant dans son champ d'application, être exercé par l'intermédiaire d'un service d'accès aux données de santé électroniques et donner lieu à une réponse immédiate. Les droits prévus par le règlement (UE) 2016/679 devraient continuer à s'appliquer, ce qui permettrait aux personnes physiques de bénéficier de leurs droits au titre des deux cadres juridiques, en particulier du droit d'obtenir une copie papier des données de santé électroniques.

(10) Il y a lieu de tenir compte du fait que l'accès immédiat des personnes physiques à certaines catégories de leurs données de santé électroniques à caractère personnel pourrait nuire à la sécurité de ces personnes physiques ou être contraire à l'éthique. Il pourrait par exemple être contraire à l'éthique d'informer un patient par voie électronique du diagnostic d'une maladie incurable susceptible de lui être fatale au lieu de fournir cette information au patient en premier lieu lors d'une consultation. Il devrait par conséquent être possible de retarder la fourniture de l'accès aux données de santé électroniques à caractère personnel dans de telles situations pour une durée limitée, par exemple jusqu'au moment où le professionnel de la santé peut expliquer la situation au patient. Les États membres devraient pouvoir établir une telle exception lorsqu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique, conformément aux limitations prévues à l'article 23 du règlement (UE) 2016/679.

(11) Le présent règlement n'affecte pas les compétences des États membres en ce qui concerne l'enregistrement initial des données de santé électroniques à caractère personnel, telles que la soumission de l'enregistrement de données génétiques au consentement de la personne physique ou à d'autres garanties. Les États membres peuvent exiger que les données soient mises à disposition sous format électronique avant l'application du présent règlement. Cela ne

devrait pas avoir d'incidence sur l'obligation de mettre à disposition sous format électronique les données de santé électroniques à caractère personnel enregistrées après la date d'application du présent règlement.

(12) Afin de compléter les informations dont elles disposent, les personnes physiques devraient avoir la possibilité d'ajouter des données de santé électroniques à leur DME ou de conserver des informations supplémentaires dans leur dossier médical personnel distinct qui pourrait être accessible aux professionnels de la santé. Toutefois, les informations introduites par les personnes physiques pourraient ne pas être aussi fiables que les données de santé électroniques saisies et vérifiées par des professionnels de la santé et elles n'ont pas la même valeur clinique ou juridique que les informations fournies par des professionnels de la santé. Les données ajoutées par des personnes physiques dans leur DME devraient donc pouvoir être clairement distinguées des données fournies par des professionnels de la santé. Cette possibilité pour les personnes physiques d'ajouter et de compléter des données de santé électroniques à caractère personnel ne devrait pas leur donner le droit de modifier les données de santé électroniques à caractère personnel qui ont été fournies par des professionnels de la santé.

(13) Permettre aux personnes physiques d'accéder plus facilement et plus rapidement à leurs données de santé électroniques à caractère personnel leur permettra de détecter d'éventuelles erreurs, telles que des informations incorrectes ou des dossiers de patients incorrectement attribués. Dans ces cas, les personnes physiques devraient pouvoir demander en ligne la rectification immédiate et gratuite des données de santé électroniques à caractère personnel incorrectes, par l'intermédiaire d'un service d'accès aux données de santé électroniques. Ces demandes de rectification devraient ensuite être traitées par les responsables du traitement concernés conformément au règlement (UE) 2016/679, en associant, si nécessaire, des professionnels de la santé ayant une spécialisation pertinente et chargés du traitement des personnes physiques.

(14) En vertu du règlement (UE) 2016/679, le droit à la portabilité des données est limité aux données traitées sur la base d'un consentement ou d'un contrat et fournies par la personne concernée à un responsable du traitement. En outre, en vertu dudit règlement, les personnes physiques ont le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre uniquement lorsque c'est techniquement possible. Le règlement (UE) 2016/679 n'impose toutefois pas d'obligation de faire en sorte que cette transmission directe soit techniquement faisable. Le droit à la portabilité des données devrait être complété dans le cadre du présent règlement, afin que les personnes physiques soient habilitées à donner l'accès à, au moins, des catégories prioritaires de leurs données de santé électroniques à caractère personnel aux professionnels de la santé de leur choix, à échanger de telles données de santé avec ces professionnels de la santé et à télécharger de telles données de santé. Les personnes physiques devraient en outre avoir le droit de demander à un prestataire de soins de santé de transmettre une partie de leurs données de santé électroniques à un destinataire clairement identifié dans le secteur de la sécurité sociale ou des services de remboursement. Ce type de transfert ne devrait être effectué que dans un sens.

(15) Le cadre défini par le présent règlement devrait s'appuyer sur le droit à la portabilité des données établi dans le règlement (UE) 2016/679, en veillant à ce que les personnes physiques, en tant que personnes concernées, puissent transmettre leurs données de santé électroniques à caractère personnel, y compris les données déduites, dans le format européen d'échange des dossiers médicaux électroniques, quelle que soit la base juridique du traitement des données de santé électroniques. Les professionnels de la santé devraient s'abstenir d'entraver l'application des droits des personnes physiques, par exemple en refusant de prendre en considération les données de santé électroniques à caractère personnel provenant d'un autre État membre et qui sont fournies dans le format européen, interopérable et fiable, d'échange des dossiers médicaux électroniques.

(16) L'accès aux dossiers médicaux électroniques par les prestataires de soins de santé ou d'autres personnes devrait être transparent pour les personnes physiques concernées. Les services d'accès aux données de santé électroniques devraient fournir des informations détaillées sur l'accès aux données, par exemple quand l'accès a eu lieu et quelle entité ou personne physique a eu accès aux données et à quelles données il a été accédé. Les personnes physiques devraient également pouvoir activer ou désactiver les notifications automatiques concernant l'accès aux données de santé électroniques à caractère personnel les concernant par l'intermédiaire des services d'accès des professionnels de la santé.

(17) Les personnes physiques pourraient ne pas vouloir qu'il soit permis d'accéder à certaines parties de leurs données de santé électroniques à caractère personnel, tout en autorisant l'accès à d'autres parties. Cela pourrait être particulièrement pertinent en cas de problèmes de santé sensibles, tels que ceux liés à la santé mentale ou sexuelle, de procédures sensibles telles que les avortements ou de données sur des médicaments spécifiques susceptibles de révéler d'autres problèmes sensibles. Il convient donc que ce partage sélectif des données de santé électroniques à caractère personnel soit soutenu et mis en œuvre au moyen de limitations fixées par la personne physique concernée de la même façon sur le territoire d'un État membre donné que pour le partage transfrontière des données. Ces limitations devraient permettre une granularité suffisante pour limiter des parties des ensembles de données, telles que des éléments des résumés des dossiers des patients. Avant de fixer les limitations, les personnes physiques devraient être informées des risques pour la sécurité des patients associés à la limitation de l'accès aux données de santé. Étant donné que l'indisponibilité des données de santé électroniques à caractère personnel faisant l'objet de limitations peut avoir une incidence sur la fourniture ou sur la qualité des services de santé délivrés à la personne physique, les personnes physiques faisant usage de telles limitations d'accès devraient assumer la responsabilité du

fait que le prestataire de soins de santé ne peut pas prendre connaissance des données au moment de fournir les services de santé. Les limitations d'accès aux données de santé électroniques à caractère personnel pourraient avoir des conséquences potentiellement mortelles et, par conséquent, l'accès à ces données devrait néanmoins être possible lorsque cela est nécessaire pour protéger des intérêts vitaux dans des situations d'urgence. Les États membres pourraient prévoir dans leur droit national des dispositions juridiques plus spécifiques sur les mécanismes de limitations placées par les personnes physiques concernant certaines parties de leurs données de santé électroniques à caractère personnel, notamment en ce qui concerne la responsabilité médicale dans les cas où les limitations ont été placées par la personne physique concernée.

(18) En outre, en raison des sensibilités différentes dans les États membres en ce qui concerne le degré de contrôle des patients sur leurs données de santé, les États membres devraient pouvoir prévoir un droit absolu pour les patients de refuser («opt-out») l'accès à leurs données de santé électroniques à caractère personnel par toute personne autre que le responsable du traitement initial, sans possibilité aucune d'outrepasser ce droit de refus dans des situations d'urgence. Dans ce cas, les États membres devraient établir les règles et les garanties spécifiques concernant ces mécanismes de refus. Ces règles et garanties spécifiques pourraient également se rapporter à des catégories spécifiques de données de santé électroniques à caractère personnel, par exemple les données génétiques. Ce droit de refus signifie que les données de santé électroniques à caractère personnel relatives à la personne physique qui exerce ce droit ne seraient pas, par l'intermédiaire des services mis en place au titre de l'EEDS, mises à la disposition d'une personne autre que le prestataire de soins de santé qui a dispensé le traitement. Les États membres devraient pouvoir exiger que les données de santé électroniques à caractère personnel soient enregistrées et conservées dans un système de DME utilisé par le prestataire de soins de santé qui a fourni les services de santé et soient accessibles uniquement à ce prestataire de soins de santé. Si une personne physique a exercé le droit de refus, les prestataires de soins de santé continueront à documenter le traitement dispensé conformément aux règles applicables et pourront accéder aux données qu'ils ont eux-mêmes enregistrées. Les personnes physiques qui exercent le droit de refus devraient pouvoir revenir sur leur décision. Dans ce cas, les données de santé électroniques à caractère personnel générées pendant la période de refus pourraient ne pas être disponibles via les services d'accès et MaSanté@UE (MyHealth@EU).

(19) L'accès rapide et total des professionnels de la santé aux dossiers médicaux des patients est fondamental pour garantir la continuité des soins, éviter les duplications et les erreurs et réduire les coûts. Cependant, par manque d'interopérabilité, dans de nombreux cas, les professionnels de la santé ne peuvent pas accéder aux dossiers médicaux complets de leurs patients et ne peuvent pas prendre des décisions médicales optimales pour leur diagnostic et leur traitement, ce qui se traduit par des coûts supplémentaires considérables pour les systèmes de santé et pour les personnes physiques et peut aboutir à des résultats de santé plus défavorables pour les personnes physiques. Les données de santé électroniques mises à disposition dans un format interopérable, et qui peuvent être transmises entre prestataires de soins de santé, peuvent aussi réduire la charge administrative que représente pour les professionnels de la santé l'introduction manuelle ou la copie des données de santé d'un système électronique à l'autre. Il y a donc lieu de doter les professionnels de la santé de moyens électroniques appropriés, tels que des dispositifs électroniques et des portails ou autres services d'accès des professionnels de la santé, pour utiliser les données de santé électroniques à caractère personnel dans l'exercice de leurs fonctions. Comme il est difficile de déterminer à l'avance et de manière exhaustive quelles données parmi les données existantes dans les catégories prioritaires sont médicalement pertinentes dans un épisode de soins spécifique, les professionnels de la santé devraient disposer d'un large accès aux données. Lorsqu'ils accèdent aux données relatives à leurs patients, les professionnels de la santé devraient se conformer au droit applicable, aux codes de conduite, aux lignes directrices déontologiques ou à d'autres dispositions régissant la conduite éthique en ce qui concerne le partage d'informations ou l'accès aux informations, en particulier dans des situations potentiellement mortelles ou extrêmes. Conformément au règlement (UE) 2016/679, afin de limiter leur accès à ce qui est pertinent dans un épisode de soins spécifique, les prestataires de soins de santé devraient suivre le principe de minimisation des données lorsqu'ils accèdent aux données de santé électroniques à caractère personnel en limitant les données auxquelles il est accédé à celles qui sont strictement nécessaires et justifiées pour un service donné. Fournir des services d'accès aux professionnels de la santé est une mission assignée par le présent règlement dans l'intérêt public, dont l'exécution nécessite le traitement de données à caractère personnel conformément à l'article 6, paragraphe 1, point e), du règlement (UE) 2016/679. Le présent règlement prévoit des conditions et des garanties pour le traitement des données de santé électroniques par le service d'accès des professionnels de la santé conformément à l'article 9, paragraphe 2, point h), du règlement (UE) 2016/679, telles que des dispositions détaillées concernant la journalisation des accès aux données de santé électroniques à caractère personnel et qui visent à assurer la transparence à l'égard des personnes concernées. Le présent règlement devrait cependant être sans préjudice du droit national en ce qui concerne le traitement des données de santé pour la fourniture de soins de santé, notamment les dispositions de droit national établissant les catégories de professionnels de la santé qui peuvent traiter différentes catégories de données de santé électroniques.

(20) Afin de faciliter l'exercice des droits complémentaires d'accès et de portabilité établis en vertu du présent règlement, les États membres devraient mettre en place un ou plusieurs services d'accès aux données de santé électroniques. Ces services pourraient être fournis au niveau national, régional ou local, ou par des prestataires de soins de santé, sous la forme d'un portail en ligne destiné aux patients, d'une application pour les appareils mobiles ou d'autres moyens. Ils

devraient être conçus pour être facilement accessibles, notamment pour les personnes handicapées. La fourniture d'un tel service, permettant aux personnes physiques d'accéder facilement à leurs données de santé électroniques à caractère personnel, est d'un intérêt public important. Le traitement des données de santé électroniques à caractère personnel par l'intermédiaire de ces services est nécessaire à l'exécution de cette mission assignée par le présent règlement au sens de l'article 6, paragraphe 1, point e), et de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679. Le présent règlement fixe les conditions et les garanties nécessaires pour le traitement des données de santé électroniques dans les services d'accès aux données de santé électroniques, telles que l'identification électronique des personnes physiques accédant à ces services.

(21) Les personnes physiques devraient pouvoir donner une autorisation à d'autres personnes physiques de leur choix, telles que leurs parents ou d'autres personnes physiques proches, permettant à ces personnes de leur choix d'accéder ou de contrôler l'accès aux données de santé électroniques à caractère personnel des personnes physiques ayant donné l'autorisation ou d'utiliser des services de santé numérique en leur nom. De telles autorisations pourraient aussi être pratiques pour d'autres utilisations par les personnes physiques ayant reçu une telle autorisation. Des services de procuration destinés à activer et à mettre en œuvre ces autorisations devraient être établis par les États membres, et ces services devraient être mis en relation avec les services d'accès aux données de santé électroniques à caractère personnel, tels que les portails ou les applications pour les appareils mobiles destinés aux patients. Ces services de procuration devraient aussi permettre aux tuteurs d'agir au nom des personnes dont ils ont la charge, y compris les mineurs; dans ce genre de situations, les autorisations pourraient être automatiques. Outre ces services de procuration, les États membres devraient également mettre en place des services d'assistance facilement accessibles, fournis par un personnel dûment formé et chargé d'aider les personnes physiques à exercer leurs droits. Afin de tenir compte des cas dans lesquels la présentation de certaines données de santé électroniques à caractère personnel de personnes à charge à leurs tuteurs pourrait être contraire aux intérêts ou à la volonté des personnes à charge, y compris des mineurs, les États membres devraient pouvoir prévoir des limitations et des garanties dans le droit national, ainsi que des mécanismes pour leur mise en œuvre technique. Les services d'accès aux données de santé électroniques à caractère personnel, tels que les portails ou les applications pour les appareils mobiles destinés aux patients, devraient utiliser ces autorisations et ainsi permettre aux personnes physiques autorisées d'accéder aux données de santé électroniques à caractère personnel relevant du champ d'application de l'autorisation. Afin de fournir une solution transversale plus conviviale, les services de procuration numériques devraient être alignés sur le règlement (UE) nº 910/2014 du Parlement européen et du Conseil [7] et sur les spécifications techniques du portefeuille européen d'identité numérique. Cet alignement contribuerait à réduire les charges tant administratives que financières pour les États membres en réduisant le risque de développer des systèmes parallèles qui ne seraient pas interopérables dans l'ensemble de l'Union.

(22) Dans certains États membres, les soins de santé sont dispensés par des équipes de gestion des soins primaires, qui sont des groupes de professionnels de la santé centrés sur les soins primaires, tels que des médecins généralistes, qui exercent leurs activités de soins primaires sur la base d'un plan de soins de santé qu'elles établissent. D'autres types d'équipes de soins de santé existent également dans plusieurs États membres pour d'autres objectifs de soins. Dans le cadre de l'utilisation primaire dans l'EEDS, l'accès devrait être fourni aux professionnels de la santé appartenant à ces équipes.

(23) Les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 sont compétentes pour surveiller l'application dudit règlement et veiller au respect de celui-ci, en particulier pour surveiller le traitement des données de santé électroniques à caractère personnel et traiter les réclamations introduites par les personnes physiques concernées. Le présent règlement établit des droits supplémentaires pour les personnes physiques en ce qui concerne l'utilisation primaire, qui vont au-delà du droit d'accès et du droit à la portabilité inscrits dans le règlement (UE) 2016/679, et qui complètent ces droits. Dès lors que ces droits supplémentaires devraient également être mis en œuvre par les autorités de contrôle instituées en vertu du règlement (UE) 2016/679, les États membres devraient veiller à ce que ces autorités de contrôle disposent des ressources financières et humaines et des locaux et infrastructures nécessaires à l'accomplissement effectif de ces tâches supplémentaires. L'autorité de contrôle ou les autorités de contrôle chargées de la surveillance et de l'exécution du traitement des données de santé électroniques à caractère personnel à des fins d'utilisation primaire en conformité avec le présent règlement devraient être compétentes pour imposer des amendes administratives. Le système juridique du Danemark ne permet pas d'imposer des amendes administratives comme le prévoit le présent règlement. Les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que, au Danemark, les amendes soient imposées par les juridictions nationales compétentes sous la forme d'une sanction pénale, à condition qu'une telle application des règles ait un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées devraient être effectives, proportionnées et dissuasives.

[7] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

(24) Les États membres devraient s'efforcer d'adhérer aux principes éthiques, tels que les principes éthiques européens en matière de santé numérique adoptés par le réseau «Santé en ligne» le 26 janvier 2022 et le principe de confidentialité entre les professionnels de la santé et leurs patients dans l'application du présent règlement. Reconnaissant l'importance des principes éthiques, les principes éthiques européens en matière de santé numérique fournissent des orientations aux praticiens, aux chercheurs, aux innovateurs, aux décideurs politiques et aux régulateurs.

(25) La pertinence des différentes catégories de données de santé électroniques pour les différents scénarios de soins de santé varie. Différentes catégories ont aussi atteint différents niveaux de maturité en matière de normalisation, et la mise en œuvre de mécanismes en vue de leur échange peut donc être plus ou moins complexe selon la catégorie. L'amélioration de l'interopérabilité et du partage de données devrait donc être progressive et il est nécessaire de hiérarchiser certaines catégories de données de santé électroniques. Les catégories de données de santé électroniques telles que les résumés des dossiers des patients, les prescriptions et les dispensations électroniques, les examens d'imagerie médicale et les comptes rendus d'imagerie médicale y afférents, les résultats d'examens médicaux, tels que les résultats de laboratoires et les comptes rendus y afférents et les rapports de sortie d'hôpital, ont été sélectionnées par le réseau «Santé en ligne» comme étant les plus pertinentes pour la majorité des situations de soins de santé et devraient être considérées comme des catégories prioritaires pour que les États membres mettent en œuvre l'accès à celles-ci et à leur transmission. Lorsque ces catégories prioritaires de données représentent des groupes de données de santé électroniques, le présent règlement devrait s'appliquer à la fois aux groupes dans leur ensemble, et aux entrées de données individuelles comprises dans ces groupes. Ainsi, étant donné que le statut vaccinal fait partie du résumé du dossier du patient, les droits et exigences liés au résumé du dossier du patient devraient également s'appliquer à ce statut vaccinal, même s'il est traité séparément du résumé du dossier du patient dans son ensemble. Lorsque de nouveaux besoins en matière d'échange de catégories supplémentaires de données de santé électroniques sont mis en évidence à des fins de soins de santé, l'accès à ces catégories supplémentaires et leur échange devraient être possible en vertu du présent règlement. Les catégories supplémentaires devraient d'abord être mises en œuvre au niveau des États membres et l'échange sur une base volontaire de telles catégories de données dans les situations transfrontières entre les États membres coopérants devrait être prévu dans le présent règlement. Il y a lieu d'accorder une attention particulière à l'échange de données dans les régions frontalières des États membres voisins où la fourniture de services de santé transfrontières est plus fréquente et nécessite des procédures encore plus rapides que dans le reste de l'Union en général.

(26) Le niveau de disponibilité des données de santé et des données génétiques à caractère personnel au format électronique varie selon les États membres. L'EEDS devrait permettre aux personnes physiques de disposer plus facilement de ces données au format électronique et de mieux contrôler l'accès à leurs données de santé électroniques à caractère personnel et le partage de ces données. De plus, cela contribuerait à la réalisation de l'objectif consistant à ce que 100 % des citoyens de l'Union aient accès à leur dossier médical électronique d'ici à 2030, conformément à la décision (UE) 2022/2481 du Parlement européen et du Conseil ([8]). Afin de rendre les données de santé électroniques accessibles et transmissibles, il convient d'accéder à ces données et de transmettre ces données dans un format européen commun interopérable d'échange de dossiers médicaux électroniques, au moins pour certaines catégories de données de santé électroniques, telles que les résumés des dossiers des patients, les ordonnances et dispensations électroniques, les examens d'imagerie médicale et les comptes rendus d'imagerie médicale y afférents, les résultats d'examens médicaux et les rapports de sortie d'hôpital, sous réserve de périodes de transition. Lorsque des données de santé électroniques à caractère personnel sont mises à la disposition d'un prestataire de soins de santé ou d'une pharmacie par une personne physique, ou sont transmises par un autre responsable du traitement dans le format européen d'échange des dossiers médicaux électroniques, ce format devrait être accepté et le destinataire devrait être en mesure de lire les données et de les utiliser pour la prestation de soins de santé ou la délivrance d'un médicament, favorisant ainsi la prestation des services de soins de santé ou la délivrance d'une ordonnance électronique. Le format européen d'échange des dossiers médicaux électroniques devrait être conçu de manière à faciliter, dans la mesure du possible, la traduction des données de santé électroniques communiquées à l'aide de ce format dans les langues officielles de l'Union. La recommandation (UE) 2019/243 de la Commission ([9]) jette les bases d'un tel format européen commun d'échange des dossiers médicaux électroniques. L'interopérabilité de l'EEDS devrait contribuer à la création d'ensembles européens de données de santé de bonne qualité. L'utilisation d'un format européen d'échange des dossiers médicaux électroniques devrait se généraliser au niveau de l'Union et au niveau national. Le format européen d'échange des dossiers médicaux électroniques pourrait permettre son utilisation par différents profils au niveau des systèmes de DME et au niveau des points de contact nationaux pour la santé numérique dans MaSanté@UE (MyHealth@EU) pour l'échange transfrontière de données.

(27) Si les systèmes de DME sont largement répandus, le niveau de numérisation des données de santé varie dans les États membres en fonction des catégories de données et de la couverture des prestataires de soins de santé qui enregistrent les données de santé au format électronique. Afin de soutenir l'application des droits des personnes concernées en matière d'accès et d'échange de données de santé électroniques, une action de l'Union est nécessaire pour éviter d'amplifier la fragmentation. Pour contribuer à la qualité et à la continuité des soins de santé, certaines catégories de données de santé devraient être enregistrées au format électronique de manière systématique et conformément aux

([8]) Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030 (JO L 323 du 19.12.2022, p. 4).

([9]) Recommandation (UE) 2019/243 de la Commission du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés (JO L 39 du 11.2.2019, p. 18).

exigences spécifiques en matière de qualité des données. Le format européen d'échange des dossiers médicaux électroniques devrait servir de base aux spécifications liées à l'enregistrement et à l'échange de données de santé électroniques.

(28) La télémédecine est un outil de plus en plus important qui permet aux patients d'avoir accès aux soins et de lutter contre les inégalités. Elle est susceptible de réduire les inégalités en matière de santé et de renforcer la libre circulation transfrontière des citoyens de l'Union. Les outils numériques et les autres outils technologiques peuvent faciliter la prestation de soins dans les régions éloignées. Lorsque des services numériques accompagnent la prestation matérielle d'un service de soins de santé, ils devraient être inclus dans la prestation de soins globale. En vertu de l'article 168 du traité sur le fonctionnement de l'Union européenne, les États membres sont responsables de leur politique de santé, en particulier de l'organisation et de la fourniture de services de santé et de soins médicaux, y compris de la réglementation d'activités telles que les pharmacies en ligne, la télémédecine et d'autres services qu'ils fournissent et remboursent, conformément à leur législation nationale. Les différentes politiques en matière de soins de santé ne devraient toutefois pas faire obstacle à la libre circulation des données de santé électroniques dans le contexte des soins de santé transfrontières, par exemple la télémédecine et les services des pharmacies en ligne.

(29) Le règlement (UE) nº 910/2014 fixe les conditions dans lesquelles les États membres procèdent à l'identification des personnes physiques dans des situations transfrontières en utilisant des moyens d'identification électronique délivrés par un autre État membre, et il établit des règles pour la reconnaissance mutuelle de ces moyens d'identification électronique. L'EEDS exige un accès sécurisé aux données de santé électroniques, y compris dans les situations transfrontières. Les services d'accès aux données de santé électroniques et les services de télémédecine devraient permettre aux personnes physiques d'exercer leurs droits indépendamment de leur État membre d'affiliation, et devraient dès lors favoriser l'identification des personnes physiques à l'aide de tout moyen d'identification électronique reconnu en vertu du règlement (UE) nº 910/2014. Compte tenu des difficultés potentielles de mise en correspondance des identités dans les situations transfrontières, il pourrait être nécessaire pour les États membres de traitement de délivrer des mécanismes d'accès complémentaires tels que des jetons ou des codes d'accès aux personnes physiques qui arrivent d'autres États membres et reçoivent des soins de santé. La Commission devrait être habilitée à adopter des actes d'exécution pour déterminer les exigences relatives à l'identification et à l'authentification interopérables et transfrontières des personnes physiques et des professionnels de la santé, y compris tout mécanisme complémentaire qui est nécessaire pour garantir que les personnes physiques peuvent exercer les droits afférents à leurs données de santé électroniques à caractère personnel dans des situations transfrontières.

(30) Les États membres devraient désigner des autorités de santé numérique compétentes pour la planification et la mise en œuvre des normes relatives à l'accès aux données de santé électroniques, à leur transmission et à l'exécution des droits des personnes physiques et des professionnels de la santé, en tant qu'organisations distinctes ou comme faisant partie d'autorités déjà existantes. Le personnel de l'autorité de santé numérique ne devrait pas détenir d'intérêts, financiers ou autres, dans des industries ou des activités économiques qui seraient de nature à compromettre son impartialité. Des autorités de santé numérique existent déjà dans la plupart des États membres et elles s'occupent des DME, de l'interopérabilité, de la sécurité ou de la normalisation. Dans l'exercice de leurs tâches, les autorités de santé numérique devraient coopérer notamment avec les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 et les organes de contrôle institués en vertu du règlement (UE) nº 910/2014. Les autorités de santé numérique peuvent également coopérer avec le Comité européen de l'intelligence artificielle institué par le règlement (UE) 2024/1689 du Parlement européen et du Conseil ([10]), le groupe de coordination en matière de dispositifs médicaux institué par le règlement (UE) 2017/745 du Parlement européen et du Conseil ([11]), le comité européen de l'innovation dans le domaine des données institué en vertu du règlement (UE) 2022/868 du Parlement européen et du Conseil ([12]) et les autorités compétentes au titre du règlement (UE) 2023/2854 du Parlement européen et du Conseil ([13]). Les États membres devraient faciliter la participation des acteurs nationaux à la coopération à l'échelle de l'Union, faciliter la transmission de l'expertise et la fourniture de conseils sur la conception des solutions nécessaires pour atteindre les objectifs de l'EEDS.

([10]) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([11]) Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1).

([12]) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

([13]) Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(31) Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne physique ou morale devrait disposer du droit à un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de santé numérique qui la concerne ou lorsqu'une autorité de santé numérique ne traite pas une réclamation ou n'informe pas la personne physique ou morale, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation. Toute action contre une autorité de santé numérique devrait être intentée devant les juridictions des États membres dans lesquels l'autorité de santé numérique est établie.

(32) Les autorités de santé numérique devraient disposer des compétences techniques suffisantes, en rassemblant éventuellement des experts de différentes organisations. Les activités des autorités de santé numérique devraient être bien organisées et contrôlées afin de garantir leur efficacité. Les autorités de santé numérique devraient prendre les mesures nécessaires pour protéger les droits des personnes physiques en mettant en place des solutions techniques nationales, régionales et locales telles que des solutions d'intermédiation pour les DME nationaux et des portails nationaux destinés aux patients. Lorsqu'elles prennent de telles mesures de protection nécessaires, les autorités de santé numérique devraient appliquer à ces solutions des normes et des spécifications communes, promouvoir l'application de ces normes et spécifications dans les procédures de marchés publics et utiliser d'autres moyens innovants, y compris le remboursement des solutions qui sont conformes aux exigences d'interopérabilité et de sécurité de l'EEDS. Les États membres devraient veiller à ce que des initiatives de formation appropriées soient prises. Il convient notamment d'informer les professionnels de la santé de leurs droits et de leurs obligations en vertu du présent règlement ainsi que de les former à cet égard. Pour mener à bien leurs tâches, les autorités de santé numérique devraient coopérer, au niveau de l'Union et au niveau national, avec d'autres entités, notamment les organismes d'assurance, les prestataires de soins de santé, les professionnels de la santé, les fabricants de systèmes de DME et d'applications de bien-être, ainsi qu'avec les autres parties prenantes du secteur de la santé ou des technologies de l'information, les entités chargées des régimes de remboursement, les organismes d'évaluation des technologies de la santé, les autorités et agences de réglementation des médicaments, les autorités chargées des dispositifs médicaux, les acheteurs et les autorités chargées de la cybersécurité ou de l'identification électronique.

(33) L'accès aux données de santé électroniques et la transmission de ces données sont importants dans les situations de soins de santé transfrontières, car ils peuvent favoriser la continuité des soins de santé lorsque des personnes physiques se rendent dans d'autres États membres ou changent de lieu de résidence. La continuité des soins et l'accès rapide aux données de santé électroniques à caractère personnel sont encore plus importants pour les résidents de régions frontalières qui franchissent fréquemment une frontière pour recevoir des soins de santé. Dans de nombreuses régions frontalières, certains services de soins de santé spécialisés pourraient être plus proches de l'autre côté de la frontière que dans le même État membre. Une infrastructure est nécessaire pour transmettre les données de santé électroniques à caractère personnel entre pays, dans des situations où une personne physique a recours aux services d'un prestataire de soins de santé établi dans un autre État membre. Il convient d'envisager l'expansion progressive d'une telle infrastructure et son financement. L'infrastructure MaSanté@UE (MyHealth@EU) a été établie à cet effet, sur la base du volontariat, dans le cadre des actions visant à atteindre les objectifs fixés dans la directive 2011/24/UE du Parlement européen et du Conseil ([14]). Grâce à MaSanté@UE (MyHealth@EU), les États membres ont commencé à offrir aux personnes physiques la possibilité de communiquer leurs données de santé électroniques à caractère personnel à des prestataires de soins de santé lorsqu'elles sont en déplacement à l'étranger. Sur la base de cette expérience, la participation des États membres à MaSanté@UE (MyHealth@EU), telle qu'elle est établie par le présent règlement, devrait être obligatoire. Les spécifications techniques de MaSanté@UE (MyHealth@EU) devraient permettre l'échange de catégories prioritaires de données de santé électroniques ainsi que des catégories supplémentaires soutenues par le format européen d'échange des dossiers médicaux électroniques. Ces spécifications devraient être définies par voie d'actes d'exécution et fondées sur les spécifications transfrontières du format européen d'échange des dossiers médicaux électroniques, complétées par d'autres spécifications en matière de cybersécurité, d'interopérabilité technique et sémantique, d'opérations et de gestion des services. Les États membres devraient être tenus d'adhérer à MaSanté@UE (MyHealth@EU), de se conformer à ses spécifications techniques et d'y connecter les prestataires de soins de santé, y compris les pharmacies, car cela est nécessaire pour permettre aux personnes physiques d'exercer leurs droits prévus dans le présent règlement d'accéder à leurs données de santé électroniques à caractère personnel et de les utiliser, quel que soit l'État membre où elles se trouvent.

(34) MaSanté@UE (MyHealth@EU) fournit une infrastructure commune aux États membres pour assurer la connectivité et l'interopérabilité de manière efficace et sécurisée afin de soutenir les soins de santé transfrontières, sans porter atteinte aux responsabilités des États membres avant et après la transmission des données de santé électroniques à caractère personnel par l'intermédiaire de cette infrastructure. Les États membres sont responsables de l'organisation de leurs points de contact nationaux pour la santé numérique et du traitement des données à caractère personnel aux fins de la fourniture de soins de santé avant et après la transmission de ces données par l'intermédiaire de MaSanté@UE (MyHealth@EU). La Commission devrait surveiller, au moyen de contrôles de conformité, le respect par les points de contact nationaux pour la santé numérique des exigences nécessaires concernant le développement technique de MaSanté@UE (MyHealth@EU), ainsi que des règles détaillées concernant la sécurité, la confidentialité et la protection des données de santé électroniques à caractère personnel. En présence d'un cas grave de non-conformité de la part d'un point de contact national pour la santé numérique, la Commission devrait être en mesure de suspendre les services affectés par la non-conformité fournis par ce point de contact national pour la santé numérique. La Commission devrait agir en tant que sous-traitant au nom des États membres au sein de MaSanté@UE

([14]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

(MyHealth@EU) et fournir des services centraux à cette dernière. Afin de garantir le respect des règles en matière de protection des données et de fournir un cadre de gestion des risques pour la transmission de données de santé électroniques à caractère personnel, les responsabilités spécifiques des États membres en tant que responsables conjoints du traitement et les obligations de la Commission en tant que sous-traitant en leur nom devraient être définies en détail par voie d'actes d'exécution. Chaque État membre est seul responsable des données et des services sur son territoire. Le présent règlement constitue la base juridique du traitement des données de santé électroniques à caractère personnel dans MaSanté@UE (MyHealth@EU) en tant que mission exécutée dans l'intérêt public, assignée par le droit de l'Union, visée à l'article 6, paragraphe 1, point e), du règlement (UE) 2016/679. Ce traitement est nécessaire à la prestation de soins de santé dans les situations transfrontières, comme indiqué à l'article 9, paragraphe 2, point h), dudit règlement.

(35) Outre les services offerts par MaSanté@UE (MyHealth@EU) pour l'échange de données de santé électroniques à caractère personnel sur la base du format européen d'échange des dossiers médicaux électroniques, d'autres services ou infrastructures supplémentaires pourraient être nécessaires, par exemple en cas d'urgences de santé publique ou lorsque l'architecture de MaSanté@UE (MyHealth@EU) ne convient pas à la mise en œuvre de certains cas d'utilisation. Parmi les exemples de tels cas d'utilisation, on peut citer les fonctionnalités d'assistance en matière de cartes de vaccination, y compris l'échange d'informations sur les plans de vaccination, ou la vérification des certificats de vaccination ou d'autres certificats liés à la santé. Ces cas d'utilisation supplémentaires seraient également importants pour introduire des fonctionnalités supplémentaires permettant de gérer les crises de santé publique, telles que le soutien à la recherche des contacts en vue de contenir les maladies infectieuses. MaSanté@UE (MyHealth@EU) devrait soutenir les échanges de données de santé électroniques à caractère personnel avec les points de contact nationaux pour la santé numérique des pays tiers et les systèmes établis à l'échelon international par des organisations internationales concernés afin de contribuer à la continuité des soins de santé. Cela est particulièrement pertinent pour les personnes qui se déplacent vers et depuis des pays tiers voisins, les pays candidats et les pays et territoires d'outre-mer associés. La connexion de ces points de contact nationaux pour la santé numérique de pays tiers à MaSanté@UE (MyHealth@EU) ainsi que l'interopérabilité avec les systèmes numériques établis au niveau international par des organisations internationales devraient être soumises à un contrôle garantissant la conformité de ces points de contact et systèmes numériques avec les spécifications techniques, les règles en matière de protection des données et les autres exigences de MaSanté@UE (MyHealth@EU). En outre, étant donné que la connexion à MaSanté@UE (MyHealth@EU) impliquera des transferts de données de santé électroniques à caractère personnel vers des pays tiers, par exemple le partage du résumé du dossier d'un patient lorsque ce patient demande à se faire soigner dans ce pays tiers, des instruments de transfert pertinents devraient être mis en place au titre du chapitre V du règlement (UE) 2016/679. La Commission devrait être habilitée à adopter des actes d'exécution pour faciliter la connexion de ces points de contact nationaux pour la santé numérique de pays tiers et de ces systèmes établis à l'échelon international par des organisations internationales à MaSanté@UE (MyHealth@EU). Lors de l'élaboration de ces actes d'exécution, la Commission devrait tenir compte des intérêts des États membres en matière de sécurité nationale.

(36) Afin de permettre un échange fluide des données de santé électroniques et de garantir le respect des droits des personnes physiques et des professionnels de la santé, les systèmes de DME commercialisés dans le marché intérieur devraient pouvoir conserver et transmettre, de manière sécurisée, des données de santé électroniques de haute qualité. C'est un objectif essentiel de l'EEDS pour garantir la libre circulation en toute sécurité des données de santé électroniques au sein de l'Union. À cette fin, il convient d'établir un système d'autoévaluation de la conformité obligatoire pour les systèmes de DME traitant une ou plusieurs catégories prioritaires de données de santé électroniques afin de remédier à la fragmentation du marché tout en garantissant une approche proportionnée. Grâce à l'autoévaluation, les systèmes de DME prouveront la conformité aux exigences en matière d'interopérabilité, de sécurité et de journalisation pour la communication de données de santé électroniques à caractère personnel établies par les deux composants logiciels obligatoires de DME harmonisés par le présent règlement, à savoir le composant logiciel d'interopérabilité européen pour les systèmes de DME et le composant logiciel de journalisation européen pour les systèmes de DME (ci-après dénommés «composants logiciels harmonisés des systèmes de DME»). Les composants logiciels harmonisés des systèmes de DME concernent principalement la transformation des données, bien qu'ils peuvent impliquer la nécessité d'exigences indirectes d'enregistrement de données et de présentation des données dans les systèmes de DME. Les spécifications techniques applicables aux composants logiciels harmonisés des systèmes de DME devraient être définies par voie d'actes d'exécution et devraient être fondées sur l'utilisation du format européen d'échange des dossiers médicaux électroniques. Les composants logiciels harmonisés des systèmes de DME devraient être conçus de manière à être réutilisables et à s'intégrer sans discontinuité avec d'autres composants au sein d'un système logiciel plus vaste. Les exigences de sécurité des composants logiciels harmonisés des systèmes de DME devraient couvrir les éléments propres aux systèmes de DME, tandis que les propriétés de sécurité plus générales devraient être soutenues par d'autres mécanismes tels que ceux prévus dans le règlement (UE) 2024/2847 du Parlement européen et du Conseil ([15]). À l'appui de ce processus, il convient de mettre en place des environnements d'essai numériques européens fournissant des procédés automatisés pour vérifier si le fonctionnement des composants logiciels harmonisés d'un système de DME est conforme aux

([15]) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

exigences fixées dans le présent règlement. À cette fin, il convient de conférer des compétences d'exécution à la Commission afin qu'elle puisse définir les spécifications communes applicables à ces environnements. La Commission devrait mettre au point le logiciel nécessaire aux environnements d'essai et le mettre à disposition en tant que source ouverte. Les États membres devraient être responsables du fonctionnement des environnements d'essai numériques car ils sont plus proches des fabricants et mieux placés pour les soutenir. Les fabricants devraient utiliser ces environnements d'essai numériques pour tester leurs produits avant de les mettre sur le marché, tout en continuant à assumer l'entière responsabilité de la conformité de leurs produits. Les résultats de l'essai devraient faire partie de la documentation technique du produit. Lorsque tout ou partie du système de DME est conforme à des normes européennes ou à des spécifications communes, la liste des normes européennes et des spécifications communes concernées devrait également figurer dans la documentation technique. Pour faciliter la comparabilité des systèmes de DME, la Commission devrait élaborer un modèle uniforme de documentation technique destinée à accompagner ces systèmes.

(37) Les systèmes de DME devraient être accompagnés d'une fiche d'information contenant des informations destinées à ses utilisateurs professionnels et d'une notice d'utilisation claire et complète, y compris dans des formats accessibles aux personnes handicapées. Si un système de DME n'est pas accompagné de ces informations, le fabricant du système de DME concerné, son mandataire et tous les autres opérateurs économiques concernés devraient être tenus d'ajouter cette fiche d'information et cette notice d'utilisation au système de DME.

(38) Alors que les systèmes de DME spécifiquement conçus par le fabricant pour être utilisés à des fins de traitement d'une ou de plusieurs catégories spécifiques de données de santé électroniques devraient être soumis à une autocertification obligatoire, les logiciels à usage général ne devraient pas être considérés comme des systèmes de DME, même lorsqu'ils sont utilisés dans un établissement de soins de santé, et ne devraient donc pas être tenus de se conformer au présent règlement. Il s'agit notamment de logiciels de traitement de texte utilisés pour rédiger des rapports qui sont ensuite intégrés dans les dossiers médicaux électroniques écrits, de logiciels médiateurs à usage général ou de logiciels de gestion de bases de données utilisés dans le cadre de solutions de stockage de données.

(39) Le présent règlement impose un système d'autoévaluation de la conformité obligatoire en ce qui concerne les composants logiciels harmonisés des systèmes de DME, afin de garantir que les systèmes de DME mis sur le marché de l'Union peuvent échanger des données dans le format européen d'échange des dossiers médicaux électroniques et qu'ils disposent des capacités de journalisation requises. Cette autoévaluation de la conformité obligatoire, qui prendrait la forme d'une déclaration UE de conformité du fabricant, devrait garantir que ces exigences sont remplies de manière proportionnée, tout en évitant de faire peser une charge inutile sur les États membres et les fabricants.

(40) Les fabricants devraient apposer sur les documents d'accompagnement du système de DME et, le cas échéant, sur son emballage un marquage CE de conformité indiquant que le système de DME est conforme au présent règlement et, en ce qui concerne les aspects non couverts par le présent règlement, à d'autres dispositions applicables du droit de l'Union qui exigent également l'apposition d'un tel marquage. Les États membres devraient s'appuyer sur les mécanismes existants pour assurer la bonne application des dispositions concernant le marquage CE de conformité au titre des dispositions pertinentes du droit de l'Union et devrait prendre les mesures nécessaires en cas d'usage abusif de ce marquage.

(41) Les États membres devraient rester compétents pour définir les exigences applicables à tout autre composant logiciel des systèmes de DME ainsi que les modalités et conditions de connexion des prestataires de soins de santé à leurs infrastructures nationales respectives, qui pourraient faire l'objet d'une évaluation par un tiers au niveau national. Afin de faciliter le bon fonctionnement du marché intérieur pour les systèmes de DME, des produits de santé numérique et des services associés, il est nécessaire d'assurer le plus possible la transparence en ce qui concerne les dispositions du droit national fixant les exigences applicables aux systèmes de DME et les dispositions relatives à l'évaluation de leur conformité en ce qui concerne les aspects autres que les composants logiciels harmonisés des systèmes de DME. Les États membres devraient dès lors informer la Commission de l'existence de ces exigences nationales afin qu'elle dispose des informations nécessaires pour s'assurer que ces exigences n'aient pas d'effets négatifs sur les composants logiciels harmonisés des systèmes de DME.

(42) Certains composants logiciels des systèmes de DME pourraient être considérés comme des dispositifs médicaux au titre du règlement (UE) 2017/745 ou comme des dispositifs médicaux de diagnostic in vitro au titre du règlement (UE) 2017/746 du Parlement européen et du Conseil ([16]). Les logiciels ou modules de logiciels qui relèvent de la définition d'un dispositif médical, d'un dispositif de diagnostic in vitro ou d'un système d'intelligence artificielle (IA) considéré à haut risque (ci-après dénommé «système d'IA à haut risque») devraient être certifiés conformément aux règlements (UE) 2017/745, (UE) 2017/746 et (UE) 2024/1689, selon le cas. Bien que ces produits soient tenus de répondre aux exigences des règlements respectifs régissant ces produits, les États membres devraient prendre les mesures appropriées pour garantir que les évaluations de la conformité respectives s'effectuent dans le cadre d'une procédure conjointe ou coordonnée afin de limiter la charge administrative sur les fabricants et les autres opérateurs économiques. Les exigences essentielles en matière d'interopérabilité du présent règlement ne devraient s'appliquer que dans la mesure où le fabricant d'un dispositif médical, d'un dispositif médical de diagnostic in vitro ou d'un système d'IA à haut risque, qui fournit des données de santé électroniques à traiter dans le cadre d'un système de

([16]) Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

DME, allègue l'interopérabilité du dispositif ou du système avec ce système de DME. Dans ce cas, les dispositions relatives aux spécifications communes des systèmes de DME devraient être applicables à ces dispositifs médicaux, ces dispositifs médicaux de diagnostic in vitro et ces systèmes d'IA à haut risque.

(43) Pour favoriser davantage l'interopérabilité et la sécurité, les États membres devraient pouvoir maintenir ou définir des règles spécifiques pour l'acquisition, le remboursement ou le financement des systèmes de DME au niveau national dans le contexte de l'organisation, de la fourniture ou du financement de services de santé. Ces règles spécifiques ne devraient pas entraver la libre circulation des systèmes de DME dans l'Union. Certains États membres ont introduit une certification obligatoire des systèmes de DME ou des tests d'interopérabilité obligatoires pour connecter ces systèmes aux services de santé numérique nationaux. Ces exigences sont généralement reflétées dans les procédures de marchés publics organisées par les prestataires de soins de santé et les autorités nationales ou régionales. La certification obligatoire des systèmes de DME à l'échelle de l'Union devrait établir une base de référence qui pourrait être utilisée dans les procédures de marchés publics au niveau national.

(44) Pour garantir aux patients l'exercice effectif des droits que leur confère le présent règlement, les prestataires de soins de santé devraient également se conformer au présent règlement lorsqu'ils élaborent et utilisent un système de DME «en interne» pour mener à bien des activités internes sans le mettre sur le marché en échange d'un paiement ou d'une rémunération. Dans ce contexte, ces prestataires de soins de santé devraient respecter toutes les exigences applicables aux fabricants en ce qui concerne ces systèmes de DME qui sont élaborés «en interne» et que ces prestataires de soins de santé mettent en service. Toutefois, comme les prestataires de soins de santé peuvent avoir besoin de plus de temps pour préparer leur mise en conformité avec le présent règlement, ces exigences ne devraient s'appliquer à ces systèmes qu'après une période transitoire prolongée.

(45) Il est nécessaire de prévoir une répartition claire et proportionnée des obligations incombant à chaque opérateur économique selon son rôle dans le processus d'approvisionnement et de distribution des systèmes de DME. Les opérateurs économiques devraient être responsables de la conformité en fonction de leurs rôles respectifs dans ce processus et devraient s'assurer qu'ils ne mettent à disposition sur le marché que des systèmes de DME qui sont conformes aux exigences pertinentes.

(46) La conformité aux exigences essentielles en matière d'interopérabilité et de sécurité devrait être démontrée par les fabricants de systèmes de DME au moyen de la mise en œuvre de spécifications communes. À cette fin, il convient de conférer des compétences d'exécution à la Commission pour déterminer ces spécifications communes concernant les ensembles de données, les systèmes de codage, les spécifications techniques, les normes, les spécifications et les profils pour l'échange de données, ainsi que les exigences et les principes liés à la sécurité des patients et à la sécurité, à la confidentialité, à l'intégrité et à la protection des données à caractère personnel, ainsi que les spécifications et les exigences liées à la gestion de l'identification et à l'utilisation de l'identification électronique. Les autorités de santé numérique devraient contribuer à l'élaboration de ces spécifications communes. Le cas échéant, ces spécifications communes devraient être fondées sur des normes harmonisées existantes pour les composants logiciels harmonisés des systèmes de DME et être compatibles avec le droit sectoriel. Lorsque les spécifications communes revêtent une importance particulière par rapport aux exigences en matière de protection des données à caractère personnel en ce qui concerne les systèmes de DME, elles devraient faire l'objet, avant leur adoption, d'une consultation du comité européen de la protection des données et du Contrôleur européen de la protection des données (CEPD), en vertu de l'article 42, paragraphe 2, du règlement (UE) 2018/1725.

(47) Afin de garantir une exécution appropriée et efficace des exigences et obligations fixées dans le présent règlement, le système de surveillance du marché et de conformité des produits établi par le règlement (UE) 2019/1020 du Parlement européen et du Conseil ([17]) devrait s'appliquer. En fonction de l'organisation définie au niveau national, ces activités de surveillance du marché pourraient être menées par les autorités de santé numérique qui veillent à la mise en œuvre correcte du chapitre II du présent règlement, ou par une autorité de surveillance du marché distincte, responsable des systèmes de DME. Bien que la désignation des autorités de santé numérique en tant qu'autorités de surveillance du marché puisse présenter des avantages pratiques importants en matière de mise en œuvre de la santé et des soins, il convient d'éviter tout conflit d'intérêts, par exemple en séparant les différentes tâches.

(48) Le personnel des autorités de surveillance du marché ne devrait avoir aucun conflit d'intérêts économiques, financiers ou personnels, direct ou indirect, qui pourrait être considéré comme préjudiciable à son indépendance et, en particulier, ne devrait pas se trouver dans une situation qui pourrait, directement ou indirectement, affecter l'impartialité de sa conduite professionnelle. Les États membres devraient définir et publier la procédure de sélection des autorités de surveillance du marché. Ils devraient veiller à ce que la procédure soit transparente et ne permette pas les conflits d'intérêts.

(49) Les utilisateurs d'applications de bien-être, y compris les applications pour les appareils mobiles, devraient être informés de la capacité de ces applications à être connectées et à fournir des données aux systèmes de DME ou aux solutions de santé électronique nationales, dans les cas où les données produites par les applications de bien-être sont utiles à des fins de soins de santé. La capacité de ces applications à exporter des données dans un format

([17]) Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011 (JO L 169 du 25.6.2019, p. 1).

interopérable est également pertinente à des fins de portabilité des données. Le cas échéant, les utilisateurs devraient être informés de la conformité de ces applications de bien-être aux exigences d'interopérabilité et de sécurité. Toutefois, étant donné le grand nombre d'applications de bien-être et la pertinence limitée, à des fins de soins de santé, des données produites par nombre d'entre elles, un système de certification ne serait pas proportionné pour ces applications. Un système de labellisation obligatoire devrait dès lors être établi pour les applications de bien-être au sujet desquelles l'interopérabilité avec les systèmes de DME est alléguée, en tant que système approprié pour offrir aux utilisateurs d'applications de bien-être la transparence en ce qui concerne la conformité aux exigences prévues dans le présent règlement, les aidant ainsi à choisir des applications de bien-être appropriées qui respectent des normes élevées d'interopérabilité et de sécurité. La Commission devrait déterminer, par voie d'actes d'exécution, les détails concernant le format et le contenu de ce label.

(50) Les États membres devraient rester libres de réglementer d'autres aspects de l'utilisation des applications de bien-être, pour autant que les règles correspondantes soient conformes au droit de l'Union.

(51) La diffusion d'informations sur les systèmes de DME certifiés et les applications de bien-être labellisées est nécessaire pour permettre aux acheteurs et aux utilisateurs de ces produits de trouver des solutions interopérables répondant à leurs besoins spécifiques. Une base de données des systèmes de DME et des applications de bien-être interopérables, qui ne relèvent pas du champ d'application des règlements (UE) 2017/745 et (UE) 2024/1689, devrait donc être établie au niveau de l'Union, similaire à la base de données européenne sur les dispositifs médicaux (Eudamed) établie par le règlement (UE) 2017/745. Les objectifs de la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être devraient être d'améliorer la transparence globale, d'éviter la pluralité des exigences en matière de rapports ainsi que de rationaliser et de faciliter le flux d'informations. Pour les dispositifs médicaux et les systèmes d'IA, l'enregistrement devrait être maintenu dans les bases de données existantes établies respectivement par les règlements (UE) 2017/745 et (UE) 2024/1689, mais la conformité aux exigences d'interopérabilité devrait être indiquée par les fabricants lorsqu'ils l'allèguent, afin de fournir des informations aux acheteurs.

(52) Sans entraver ou remplacer les arrangements contractuels ou autres mécanismes existants, le présent règlement vise à établir un mécanisme commun d'accès aux données de santé électroniques à des fins d'utilisation secondaire dans l'ensemble de l'Union. Dans le cadre de ce mécanisme, les détenteurs de données de santé devraient mettre à disposition les données qu'ils détiennent sur la base d'une autorisation de traitement de données ou d'une demande de données de santé. Pour le traitement des données de santé électroniques à des fins d'utilisation secondaire, une des bases juridiques visées à l'article 6, paragraphe 1, point a), c), e) ou f), du règlement (UE) 2016/679, lu en combinaison avec l'article 9, paragraphe 2, dudit règlement, est requise. Le présent règlement fournit, dès lors, une base juridique pour l'utilisation secondaire des données de santé électroniques à caractère personnel, y compris les garanties requises au titre de l'article 9, paragraphe 2, points g), à j), du règlement (UE) 2016/679 pour permettre le traitement de catégories spéciales de données, en matière de fins licites, de gouvernance fiable de l'accès aux données de santé par la participation d'organismes responsables de l'accès aux données de santé, et de traitement dans un environnement de traitement sécurisé, ainsi que de modalités de traitement des données, énoncées dans l'autorisation de traitement de données. Les États membres ne devraient dès lors plus pouvoir maintenir ou introduire, en vertu de l'article 9, paragraphe 4, du règlement (UE) 2016/679, d'autres conditions, y compris des limitations et des dispositions spécifiques exigeant le consentement des personnes physiques en ce qui concerne le traitement à des fins d'utilisation secondaire des données de santé électroniques à caractère personnel au titre du présent règlement, à l'exception de l'introduction de mesures plus strictes et de garanties supplémentaires au niveau national visant à préserver le caractère sensible et la valeur de certaines données comme prévu dans le présent règlement. Les demandeurs de données de santé devraient également démontrer l'existence d'une base juridique, visée à l'article 6 du règlement (UE) 2016/679, qui leur permette de demander l'accès aux données de santé électroniques en vertu du présent règlement et devraient remplir les conditions énoncées au chapitre IV du présent règlement. En outre, l'organisme responsable de l'accès aux données de santé devrait évaluer les informations fournies par le demandeur de données de santé, sur la base desquelles il devrait être en mesure de délivrer une autorisation de traitement de données pour le traitement des données de santé électroniques à caractère personnel en vertu du présent règlement qui devrait satisfaire aux exigences et aux conditions énoncées au chapitre IV du présent règlement. Pour le traitement des données de santé électroniques détenues par les détenteurs de données de santé, le présent règlement crée l'obligation légale, au sens de l'article 6, paragraphe 1, point c), du règlement (UE) 2016/679, conformément à l'article 9, paragraphe 2, points i) et j), dudit règlement, pour le détenteur de données de santé de mettre les données de santé électroniques à caractère personnel à la disposition des organismes responsables de l'accès aux données de santé, tandis que la base juridique de la finalité du traitement initial, par exemple la fourniture de soins de santé, n'est pas affectée. Le présent règlement attribue également des missions d'intérêt public au sens de l'article 6, paragraphe 1, point e), du règlement (UE) 2016/679 aux organismes responsables de l'accès aux données de santé, et répond aux conditions de l'article 9, paragraphe 2, points g) à j), selon le cas, dudit règlement. Si l'utilisateur de données de santé s'appuie sur une base juridique énoncée à l'article 6, paragraphe 1, point e) ou f), du règlement (UE) 2016/679, le présent règlement devrait prévoir les garanties requises en vertu de l'article 9, paragraphe 2, du règlement (UE) 2016/679.

(53) Les données de santé électroniques utilisées à des fins d'utilisation secondaire peuvent apporter de grands avantages à la société. Il convient d'encourager l'adoption de données réelles et de données probantes réelles, y compris les résultats rapportés par les patients, à des fins réglementaires et politiques fondées sur des données probantes ainsi qu'à des fins de recherche, d'évaluation des technologies de la santé et à des fins d'objectifs cliniques. Les données réelles et les données probantes réelles sont susceptibles de compléter les données de santé actuellement mises à disposition. Pour atteindre cet objectif, il importe que les ensembles de données mis à disposition à des fins d'utilisation secondaire en vertu du présent règlement soient aussi complets que possible. Le présent règlement fournit les garanties nécessaires pour atténuer certains risques liés à la réalisation de ces avantages. L'utilisation secondaire des données de santé électroniques est fondée sur des données pseudonymisées ou anonymisées, afin d'empêcher l'identification des personnes concernées.

(54) Afin de concilier le besoin des utilisateurs de données de santé de disposer d'ensembles de données exhaustifs et représentatifs et le besoin d'autonomie des personnes physiques par rapport à leurs données de santé électroniques à caractère personnel qui sont considérées comme particulièrement sensibles, les personnes physiques devraient pouvoir prendre une décision quant à savoir si leurs données de santé électroniques à caractère personnel peuvent être traitées à des fins d'utilisation secondaire au titre du présent règlement, sous la forme d'un droit de refuser la mise à disposition de ces données à des fins d'utilisation secondaire. Il convient de prévoir un mécanisme pour exercer ce droit de refus facilement compréhensible et accessible. En outre, il est impératif de fournir aux personnes physiques des informations suffisantes et complètes sur leur droit de refus, y compris sur les avantages et les inconvénients liés à l'exercice de ce droit. Les personnes physiques ne devraient pas être tenues de donner des motifs de refus et devraient avoir la possibilité de reconsidérer leur choix à tout moment. Toutefois, pour certaines finalités étroitement liées à l'intérêt public, telles que les activités de protection contre les menaces transfrontières graves pour la santé ou la recherche scientifique pour des motifs importants d'intérêt public, il convient de prévoir la possibilité pour les États membres d'établir, en tenant compte de leur contexte national, des mécanismes permettant d'accéder aux données de santé électroniques à caractère personnel des personnes physiques qui ont exercé leur droit de refus, afin de garantir que des ensembles complets de données puissent être mis à disposition dans ces situations. De tels mécanismes devraient être conformes aux exigences établies pour l'utilisation secondaire en vertu du présent règlement. La recherche scientifique pour des motifs importants d'intérêt public pourrait, par exemple, inclure la recherche visant à répondre à des besoins médicaux non satisfaits, y compris concernant des maladies rares, ou à des menaces émergentes pour la santé. Les règles relatives à ces dérogations devraient respecter l'essence des droits et libertés fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour répondre à l'intérêt public par rapport à des objectifs scientifiques et sociétaux légitimes. Ces dérogations ne devraient être accessibles qu'aux utilisateurs de données de santé qui sont des organismes du secteur public, ou des institutions, organes ou organismes de l'Union compétents, chargés d'exécuter des tâches dans le domaine de la santé publique, ou à d'autres entités chargées d'exécuter des tâches de nature publique dans le domaine de la santé publique, ou agissant au nom ou à la demande d'une autorité publique, et uniquement si les données ne peuvent être obtenues par d'autres moyens en temps utile et de manière efficace. Ces utilisateurs de données de santé devraient justifier que le recours à une dérogation est nécessaire pour une demande individuelle d'accès à des données de santé ou une demande individuelle de données de santé. Lorsqu'une telle dérogation est appliquée, les utilisateurs de données de santé devraient continuer d'appliquer les garanties prévues au chapitre IV, notamment l'interdiction de réidentifier ou de tenter de réidentifier les personnes physiques concernées.

(55) Dans le contexte de l'EEDS, les données de santé électroniques existent déjà et sont collectées par, entre autres, des prestataires de soins de santé, des organisations professionnelles, des institutions publiques, des organismes de réglementation, des chercheurs et des assureurs dans le cadre de leurs activités. Ces données devraient également être mises à disposition à des fins d'utilisation secondaire, c'est-à-dire pour traiter des données à des fins autres que celles pour lesquelles elles ont été collectées ou produites; toutefois, beaucoup de ces données ne sont pas mises à disposition pour un traitement à ces fins. Cela limite la capacité des chercheurs, des innovateurs, des décideurs politiques, des organismes de réglementation et des médecins à utiliser ces données à des fins différentes, notamment la recherche, l'innovation, l'élaboration de politiques, la réglementation, la sécurité des patients ou la médecine personnalisée. Afin d'exploiter pleinement les avantages de l'utilisation secondaire, tous les détenteurs de données de santé devraient contribuer à cet effort en mettant à disposition à des fins d'utilisation secondaire les différentes catégories de données de santé électroniques qu'ils détiennent, sous réserve que cet effort soit toujours mis en œuvre au moyen de processus efficaces et sécurisés, et dans le respect des obligations professionnelles, telles que les obligations de confidentialité.

(56) Les catégories de données de santé électroniques pouvant être traitées à des fins d'utilisation secondaire devraient être suffisamment larges et flexibles pour s'adapter à l'évolution des besoins des utilisateurs de données de santé, tout en restant limitées à des données liées à la santé ou connues pour avoir une influence sur la santé. Il peut également s'agir de données pertinentes provenant du système de santé, par exemple, des dossiers médicaux électroniques, des données relatives aux demandes de remboursement, des données relatives aux dispensations, des données des registres de maladies ou des données génomiques, ainsi que de données ayant une incidence sur la santé, par exemple, des données sur la consommation de différentes substances, le statut ou le comportement socioéconomique, et des données sur les facteurs environnementaux tels que la pollution, le rayonnement ionisant ou l'utilisation de certaines substances chimiques. Les catégories de données de santé électroniques à des fins

d'utilisation secondaire comprennent certaines catégories de données initialement collectées à d'autres fins, telles que la recherche, les statistiques, la sécurité des patients, les activités réglementaires ou l'élaboration des politiques, par exemple, les registres d'élaboration des politiques ou les registres concernant les effets secondaires des médicaments ou des dispositifs médicaux. Des bases de données européennes qui facilitent l'utilisation ou la réutilisation des données sont disponibles dans certains domaines, tels que le cancer (le système européen d'information sur le cancer) ou les maladies rares (par exemple, la plateforme européenne d'enregistrement des maladies rares et les registres des réseaux européens de référence). Les catégories de données de santé électroniques qui peuvent être traitées à des fins d'utilisation secondaire devraient également inclure les données provenant de dispositifs médicaux générées automatiquement et les données générées par des personnes, telles que des données provenant d'applications de bien-être. Les données relatives aux essais et investigations cliniques devraient aussi être incluses dans les catégories de données de santé électroniques à des fins d'utilisation secondaire une fois que l'essai ou l'investigation cliniques a pris fin, sans que cela n'affecte le partage volontaire des données par les promoteurs des essais et investigations en cours. Les données de santé électroniques à des fins d'utilisation secondaire devraient être mises à disposition de préférence dans un format électronique structuré facilitant leur traitement par des systèmes informatiques. Parmi les exemples de formats électroniques structurés figurent des enregistrements dans une base de données relationnelle, des documents XML ou des fichiers CSV et des textes libres, des fichiers audio, des vidéos et des images fournis sous forme de fichiers lisibles par ordinateur.

(57) Les utilisateurs de données de santé qui bénéficient de l'accès aux ensembles de données prévus dans le présent règlement pourraient enrichir les données dans ces ensembles de données par diverses corrections, annotations et autres améliorations, par exemple en complétant les données manquantes ou incomplètes, améliorant ainsi l'exactitude, l'exhaustivité ou la qualité des données dans les ensembles de données. Les utilisateurs de données de santé devraient être encouragés à signaler aux organismes responsables de l'accès aux données de santé les erreurs critiques figurant dans les ensembles de données. Afin de renforcer l'amélioration de la base de données initiale et l'utilisation ultérieure de l'ensemble de données enrichi, les États membres devraient pouvoir établir des règles relatives au traitement et à l'utilisation des données de santé électroniques contenant des améliorations liées au traitement de ces données. L'ensemble de données amélioré devrait être mis gratuitement à la disposition du détenteur de données de santé d'origine, avec une description des améliorations. Le détenteur de données de santé devrait mettre à disposition le nouvel ensemble de données, à moins qu'il n'adresse une notification justifiée à l'organisme responsable de l'accès aux données de santé, par exemple dans les cas où l'enrichissement par l'utilisateur de données de santé est de mauvaise qualité. Il convient de veiller à ce que les données de santé électroniques à caractère non personnel soient disponibles à des fins d'utilisation secondaire. En particulier, les données génomiques sur les agents pathogènes ont une valeur importante pour la santé humaine, comme cela a été montré durant la pandémie de COVID-19, pendant laquelle l'accès rapide à ces données et leur partage se sont avérés essentiels pour l'élaboration rapide d'outils de détection, de contre-mesures médicales et de réactions aux menaces pour la santé publique. Le plus grand bénéfice des efforts en matière de données génomiques sur les agents pathogènes sera atteint lorsque la santé publique et les processus de recherche partageront les ensembles de données et collaboreront pour s'informer et s'améliorer mutuellement.

(58) Afin d'accroître l'efficacité de l'utilisation secondaire des données de santé électroniques à caractère personnel et d'exploiter pleinement le potentiel offert par le présent règlement, la disponibilité, dans l'EEDS, des données de santé électroniques décrites au chapitre IV devrait être telle que les données soient aussi accessibles, de qualité, prêtes et appropriées que possible aux fins de la création d'une valeur et d'une qualité scientifiques, innovantes et sociétales. Les travaux relatifs à la mise en œuvre de l'EEDS et à d'autres améliorations des ensembles de données devraient être menés en accordant la priorité aux ensembles de données qui sont les plus appropriés pour créer une telle valeur et une telle qualité.

(59) Les entités publiques ou privées reçoivent souvent un financement public, provenant de fonds nationaux ou de l'Union, pour collecter et traiter des données de santé électroniques à des fins de recherche, de statistiques officielles ou non, ou à d'autres fins similaires, y compris dans des domaines où la collecte de ces données est fragmentée ou difficile, comme en ce qui concerne les maladies rares ou le cancer. Ces données, collectées et traitées par les détenteurs de données de santé avec le soutien de fonds publics nationaux ou de l'Union, devraient être mises à la disposition des organismes responsables de l'accès aux données de santé, afin de maximiser les effets de l'investissement public et de soutenir la recherche, l'innovation, la sécurité des patients ou l'élaboration de politiques au bénéfice de la société. Dans certains États membres, les entités privées, notamment les prestataires de soins de santé privés et les organisations professionnelles, jouent un rôle central dans le secteur de la santé. Les données de santé détenues par ces prestataires devraient également être mises à disposition à des fins d'utilisation secondaire. Dans le cadre de l'utilisation secondaire, les détenteurs de données de santé devraient dès lors être des entités qui sont des prestataires de soins de santé ou des prestataires de soins ou qui mènent des recherches dans les secteurs des soins de santé ou des soins, ou qui développent des produits ou des services destinés aux secteurs des soins de santé ou des soins. Ces entités peuvent être publiques, à but non lucratif ou privées. Conformément à cette définition, les maisons de repos, les centres de jour, les entités fournissant des services aux personnes handicapées, les entités ayant des activités commerciales et technologiques liées aux soins, telles que l'orthopédie, et les entreprises fournissant des services de soins devraient être considérées comme des détenteurs de données de santé. Les personnes morales qui développent des applications de bien-être devraient également être considérées comme des détenteurs de données de santé. Les institutions, organes et organismes de l'Union qui traitent ces catégories de données de santé et de soins de santé, ainsi que les registres de mortalité, devraient également être considérés comme des détenteurs de données de santé. Afin d'éviter une charge disproportionnée pour les personnes physiques et les microentreprises, celles-ci devraient, en règle générale, être exemptées des obligations qui incombent aux détenteurs de données de santé. Les

États membres devraient toutefois pouvoir étendre les obligations des détenteurs de données de santé aux personnes physiques et aux microentreprises dans leur droit national. Afin de réduire la charge administrative, et à la lumière des principes d'efficacité et d'efficience, les États membres devraient pouvoir exiger, dans leur droit national, que des entités d'intermédiation de données de santé exécutent les obligations de certaines catégories de détenteurs de données de santé. Ces entités d'intermédiation de données de santé devraient être des personnes morales capables de traiter, de mettre à disposition, d'enregistrer et d'échanger des données de santé électroniques, fournies par les détenteurs de données, à des fins d'utilisation secondaire, et de fournir ou limiter l'accès à ces données. Ces entités d'intermédiation de données de santé effectuent des tâches qui diffèrent de celles effectuées par les services d'intermédiation de données prévus dans le règlement (UE) 2022/868.

(60) Les données de santé électroniques protégées par des droits de propriété intellectuelle ou des secrets d'affaires, y compris les données relatives aux essais, investigations et études cliniques, peuvent être très utiles pour une utilisation secondaire et favoriser l'innovation au sein de l'Union au profit des patients de l'Union. Afin d'encourager l'Union à continuer à jouer un rôle moteur dans ce domaine, il importe d'encourager le partage des données relatives aux essais et investigations cliniques par l'intermédiaire de l'EEDS à des fins d'utilisation secondaire. Les données relatives aux essais et investigations cliniques devraient être mises à disposition dans la mesure du possible, tout en prenant toutes les précautions nécessaires pour protéger les droits de propriété intellectuelle et les secrets d'affaires. Le présent règlement ne devrait pas être utilisé pour réduire ou contourner cette protection et devrait être cohérent avec les dispositions pertinentes en matière de transparence prévues par le droit de l'Union, y compris celles prévues pour les données relatives aux essais et investigations cliniques. Les organismes responsables de l'accès aux données de santé devraient évaluer comment préserver cette protection tout en permettant aux utilisateurs de données de santé d'accéder à ces données dans la mesure du possible. Si un organisme responsable de l'accès aux données de santé n'est pas en mesure de donner accès à ces données, il devrait en informer l'utilisateur des données de santé et lui expliquer pourquoi il n'est pas possible de lui donner accès à ces données. Les mesures juridiques, organisationnelles et techniques visant à protéger les droits de propriété intellectuelle ou les secrets d'affaires pourraient inclure des dispositions contractuelles communes sur l'accès aux données de santé électroniques, des obligations spécifiques dans le cadre de l'autorisation de traitement de données concernant ces droits, le prétraitement des données pour générer des données dérivées à même de protéger un secret d'affaires tout en ayant une utilité pour l'utilisateur de données, ou la configuration de l'environnement de traitement sécurisé de sorte que ces données ne soient pas accessibles à l'utilisateur des données de santé.

(61) L'utilisation secondaire des données de santé au titre de l'EEDS devrait permettre aux entités publiques, privées et à but non lucratif, ainsi qu'aux chercheurs à titre individuel, d'avoir accès aux données de santé à des fins de recherche, d'innovation, d'élaboration de politiques, d'activités éducatives, de sécurité des patients, d'activités réglementaires ou de médecine personnalisée, conformément aux finalités prévues par le présent règlement. L'accès aux données à des fins d'utilisation secondaire devrait contribuer à l'intérêt général de la société. En particulier, l'utilisation secondaire des données de santé à des fins de recherche et de développement devrait contribuer à bénéficier à la société sous la forme de nouveaux médicaments, de dispositifs médicaux, de produits et services de soins de santé à des prix abordables et équitables pour les citoyens de l'Union ainsi qu'à améliorer l'accès à ces produits et services et leur disponibilité dans tous les États membres. Les activités pour lesquelles l'accès est licite dans le cadre du présent règlement pourraient inclure l'utilisation des données de santé électroniques en vue de tâches accomplies par des organismes du secteur public, tel que l'exercice d'une fonction publique, y compris la surveillance de la santé publique, la planification et l'établissement de rapports, l'élaboration de la politique de santé et la garantie de la sécurité des patients, la qualité des soins et la durabilité des systèmes de soins de santé. Les organismes du secteur public ainsi que les institutions, organes et organismes de l'Union pourraient avoir besoin d'accéder régulièrement aux données de santé électroniques pendant une période étendue, notamment pour mener à bien leur mandat, comme prévu par le présent règlement. Les organismes du secteur public pourraient mener des activités de recherche en faisant appel à des tiers, y compris des sous-traitants, pour autant que l'organisme du secteur public reste à tout moment le superviseur de ces activités. La fourniture des données devrait également soutenir les activités liées à la recherche scientifique. La notion couverte par l'expression «à des fins de recherche scientifique» devrait être interprétée de manière large, et comprendre le développement et la démonstration technologiques, la recherche fondamentale, la recherche appliquée et la recherche financée par des fonds privés. Les activités liées à la recherche scientifique comprennent des activités d'innovation, telles que l'entraînement des algorithmes d'IA qui pourraient être utilisés dans les soins de santé ou les soins aux personnes physiques, ainsi que l'évaluation et la poursuite du développement d'algorithmes et de produits existants à de telles fins. Il est nécessaire que l'EEDS contribue aussi à la recherche fondamentale, et bien que ses avantages pour les utilisateurs finals et les patients pourraient être moins directs, cette recherche fondamentale est essentielle pour atteindre des avantages sociétaux à plus long terme. Dans certains cas, les informations de certaines personnes physiques, telles que les informations génomiques de personnes physiques atteintes d'une certaine maladie, pourraient jouer un rôle s'agissant du diagnostic ou du traitement d'autres personnes physiques. Il est nécessaire que les organismes du secteur public aillent au-delà du champ d'application du «besoin exceptionnel» du chapitre V du règlement (UE) 2023/2854. Toutefois, les organismes responsables de l'accès aux données de santé devraient être autorisés à soutenir les organismes du secteur public quand il s'agit de traiter ou de relier des données. Le présent règlement offre aux organismes du secteur public un moyen d'accéder aux informations dont ils ont besoin pour remplir les missions qui leur incombent en vertu de la loi, mais n'étend pas leur mandat.

(62) Toute tentative d'utiliser les données de santé électroniques pour mettre en place des mesures préjudiciables aux personnes physiques, telles qu'augmenter les primes d'assurance, exercer des activités potentiellement préjudiciables aux personnes physiques dans les domaines de l'emploi, des pensions ou de la banque, y compris l'hypothèque de biens immobiliers, faire de la publicité pour des produits ou des traitements, automatiser la prise de décision individuelle, réidentifier des personnes physiques ou développer des produits nocifs, devrait être interdite. Cette interdiction devrait aussi s'appliquer aux activités contraires aux dispositions éthiques prévues par le droit national, à l'exception des dispositions éthiques relatives au consentement au traitement des données à caractère personnel et des dispositions éthiques relatives au droit de refus, dès lors que le présent règlement prime sur le droit national conformément au principe général de primauté du droit de l'Union. Il devrait également être interdit de donner accès aux données de santé électroniques à des tiers non mentionnés dans l'autorisation de traitement de données ou de les mettre à la disposition de ces tiers. L'identité des personnes autorisées, notamment celle de l'investigateur principal, qui auront le droit en vertu du présent règlement d'accéder aux données de santé électroniques dans l'environnement de traitement sécurisé, devrait être indiquée dans l'autorisation de traitement de données. Les investigateurs principaux sont les personnes responsables au premier chef pour demander l'accès aux données de santé électroniques et pour traiter les données demandées dans l'environnement de traitement sécurisé pour le compte de l'utilisateur de données de santé.

(63) Le présent règlement ne devrait pas créer une habilitation en vue de l'utilisation secondaire de données de santé à des fins répressives. La prévention, la détection ou la poursuite d'infractions pénales et les enquêtes en la matière, ou l'exécution de sanctions pénales par les autorités compétentes ne devraient pas figurer parmi les finalités d'utilisation secondaire couvertes par le présent règlement. Les juridictions et autres entités du système judiciaire ne devraient par conséquent pas être considérées comme des utilisateurs de données de santé pour ce qui concerne l'utilisation secondaire des données de santé au titre du présent règlement. Les juridictions et autres entités du système judiciaire ne devraient, par ailleurs, pas entrer dans la définition des détenteurs de données de santé et ne devraient donc pas être les destinataires des obligations qui incombent aux détenteurs de données de santé en vertu du présent règlement. En outre, les pouvoirs des autorités compétentes en matière de prévention, de détection et de poursuite des infractions pénales et d'enquêtes en la matière, établis par la loi pour obtenir des données de santé électroniques ne sont pas affectés par le présent règlement. De même, les données de santé électroniques détenues par les juridictions aux fins de procédures judiciaires n'entrent pas dans le champ d'application du présent règlement.

(64) La création d'un ou de plusieurs organismes responsables de l'accès aux données de santé, favorisant l'accès aux données de santé électroniques dans les États membres, est essentielle pour promouvoir l'utilisation secondaire des données liées à la santé. Les États membres devraient donc créer un ou plusieurs organismes responsables de l'accès aux données de santé, pour refléter, entre autres, leur structure constitutionnelle, organisationnelle et administrative. Toutefois, s'il existe plus d'un organisme responsable de l'accès aux données de santé, l'un d'entre eux devrait être désigné comme coordonnateur. Si un État membre crée plusieurs organismes responsables de l'accès aux données de santé, il devrait établir des règles au niveau national pour garantir la coordination de la participation de ces organismes au comité de l'espace européen des données de santé (ci-après dénommé «comité de l'EEDS»). Ledit État membre devrait en particulier désigner un organisme responsable de l'accès aux données de santé pour servir de point de contact unique, permettant une participation efficace de ces organismes, et pour assurer une coopération rapide et aisée avec les autres organismes responsables de l'accès aux données de santé, le comité de l'EEDS et la Commission. L'organisation et la taille des organismes responsables de l'accès aux données de santé pourraient varier, allant d'une organisation consacrée à part entière à une unité ou un service d'une organisation existante. Les organismes responsables de l'accès aux données de santé ne devraient pas être influencés dans leurs décisions concernant l'accès à des données électroniques à des fins d'utilisation secondaire et devraient éviter tout conflit d'intérêts. Les membres des organes de gouvernance et de décision de chaque organisme responsable de l'accès aux données de santé et leur personnel devraient donc s'abstenir de tout acte incompatible avec leurs fonctions et n'exercer aucune activité professionnelle incompatible. Toutefois, l'indépendance des organismes responsables de l'accès aux données de santé ne devrait pas signifier qu'ils ne peuvent pas être soumis à des mécanismes de contrôle ou de surveillance concernant leurs dépenses financières ou à un contrôle judiciaire. Il convient que chaque organisme responsable de l'accès aux données de santé soit doté des moyens financiers, techniques et humains, ainsi que des locaux et des infrastructures nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à la coopération avec d'autres organismes responsables de l'accès aux données de santé dans l'ensemble de l'Union. Les membres des organes de gouvernance et de décision des organismes responsables de l'accès aux données de santé et leur personnel devraient avoir les qualifications, l'expérience et les compétences nécessaires. Chaque organisme responsable de l'accès aux données de santé devrait disposer d'un budget annuel public propre, qui pourrait faire partie du budget global national ou d'une entité fédérée. Afin d'améliorer l'accès aux données de santé, et en complément de l'article 7, paragraphe 2, du règlement (UE) 2022/868, les États membres devraient conférer aux organismes responsables de l'accès aux données de santé des pouvoirs leur permettant de prendre des décisions concernant l'accès aux données de santé et leur utilisation secondaire. Il pourrait s'agir d'attribuer de nouvelles tâches aux organismes compétents désignés par les États membres en vertu de l'article 7, paragraphe 1, du règlement (UE) 2022/868 ou de désigner des organismes sectoriels, existants ou nouveaux, chargés de ces tâches en matière d'accès aux données de santé.

(65) Les organismes responsables de l'accès aux données de santé devraient surveiller l'application du chapitre IV du présent règlement et contribuer à son application cohérente dans l'ensemble de l'Union. À cet effet, les organismes responsables de l'accès aux données de santé devraient coopérer entre elles et avec la Commission. Les organismes responsables de l'accès aux données de santé devraient également coopérer avec les parties prenantes, notamment les organisations de patients. Les organismes responsables de l'accès aux données de santé devraient soutenir les

détenteurs de données de santé qui sont des petites entreprises conformément à la recommandation 2003/361/CE de la Commission ([18]), en particulier les médecins et les pharmacies. Étant donné que l'utilisation secondaire des données de santé suppose le traitement de données à caractère personnel concernant la santé, les dispositions pertinentes des règlements (UE) 2016/679 et (UE) 2018/1725 s'appliquent et les autorités de contrôle prévues par ces règlements devraient rester les seules autorités compétentes pour faire respecter ces dispositions. Les organismes responsables de l'accès aux données de santé devraient informer les autorités chargées de la protection des données de toute sanction imposée et de tout problème potentiel lié au traitement des données à des fins d'utilisation secondaire et échanger toute information pertinente dont ils disposent pour garantir l'exécution des règles pertinentes. Outre les tâches nécessaires pour garantir une utilisation secondaire des données de santé efficace, les organismes responsables de l'accès aux données de santé devraient s'efforcer d'augmenter la disponibilité d'ensembles de données de santé supplémentaires et de promouvoir l'élaboration de normes communes. Ils devraient appliquer des techniques de pointe éprouvées garantissant que les données de santé électroniques sont traitées de manière à préserver la confidentialité des informations contenues dans les données dont l'utilisation secondaire est autorisée, notamment les techniques de pseudonymisation, d'anonymisation, de généralisation, de suppression et de randomisation des données à caractère personnel. Les organismes responsables de l'accès aux données de santé peuvent préparer des ensembles de données pour l'utilisateur des données de santé conformément à l'autorisation de traitement de données délivrée. À cet égard, les organismes responsables de l'accès aux données de santé devraient coopérer par-delà les frontières pour développer et échanger des bonnes pratiques et des techniques. Cela inclut des règles de pseudonymisation et d'anonymisation des ensembles de microdonnées. Le cas échéant, la Commission devrait fixer les procédures et les exigences, et prévoir les outils techniques en vue d'une procédure unifiée de pseudonymisation et d'anonymisation des données de santé électroniques.

(66) Les organismes responsables de l'accès aux données de santé devraient garantir que l'utilisation secondaire est transparente en fournissant des informations publiques sur les autorisations de traitement de données délivrées et leurs justifications, les mesures prises pour protéger les droits des personnes physiques, les moyens dont disposent les personnes physiques pour exercer leurs droits en ce qui concerne l'utilisation secondaire, et les résultats de l'utilisation secondaire, notamment via des liens vers des publications scientifiques. Ces informations sur les résultats de l'utilisation secondaire devraient également inclure, le cas échéant, un résumé à l'intention des profanes, à fournir par l'utilisateur de données de santé. Ces obligations de transparence complètent les obligations prévues à l'article 14 du règlement (UE) 2016/679. Les exceptions prévues à l'article 14, paragraphe 5, dudit règlement pourraient s'appliquer. Lorsque de telles exceptions s'appliquent, les obligations de transparence établies par le présent règlement devraient contribuer à garantir un traitement équitable et transparent, tel qu'il est visé à l'article 14, paragraphe 2, du règlement (UE) 2016/679, par exemple par la fourniture d'informations sur la finalité du traitement et les catégories de données traitées, de sorte que les personnes physiques puissent comprendre si leurs données sont mises à disposition à des fins d'utilisation secondaire en vertu d'autorisations de traitement de données.

(67) Les personnes physiques devraient être informées, par les détenteurs de données de santé, des constatations importantes liées à leur santé faites par les utilisateurs de données de santé. Les personnes physiques devraient avoir le droit de demander à ne pas être informées de ces constatations. Les États membres pourraient fixer des conditions sur les modalités de fourniture de telles informations par les détenteurs de données de santé aux personnes physiques concernées et sur l'exercice du droit de ne pas être informé. Conformément à l'article 23, paragraphe 1, point i), du règlement (UE) 2016/679, les États membres devraient pouvoir limiter la portée de l'obligation d'informer les personnes physiques chaque fois que cela est nécessaire pour assurer leur protection sur la base de la sécurité des patients et de l'éthique, en retardant la communication de leurs informations jusqu'à ce qu'un professionnel de la santé puisse communiquer et expliquer aux personnes physiques concernées les informations qui peuvent potentiellement avoir une incidence sur leur santé.

(68) Afin de promouvoir la transparence, les organismes responsables de l'accès aux données de santé devraient également publier des rapports d'activité, tous les deux ans, donnant une vue d'ensemble de leurs activités. Lorsqu'un État membre a désigné plus d'un organisme responsable de l'accès aux données de santé, l'organisme de coordination devrait élaborer et publier un rapport commun tous les deux ans. Les rapports d'activité devraient adopter une structure convenue au sein du comité de l'EEDS et donner une vue d'ensemble des activités, y compris des informations sur les décisions relatives aux demandes, aux audits et au dialogue avec les parties prenantes concernées. Ces parties prenantes peuvent comprendre des représentants de personnes physiques, des organisations de patients, des professionnels de la santé, des chercheurs et des comités d'éthique.

(69) Afin de favoriser l'utilisation secondaire, les détenteurs de données de santé devraient s'abstenir de retenir les données, de demander des redevances injustifiées qui ne sont ni transparentes ni proportionnées aux coûts de mise à disposition des données ou, le cas échéant, aux coûts marginaux de collecte des données, de demander aux utilisateurs de données de santé de copublier la recherche ou d'autres pratiques qui pourraient dissuader les utilisateurs de données de santé de demander les données. Lorsqu'un détenteur de données de santé est un organisme du secteur public, la partie des redevances associée à ses coûts ne devrait pas couvrir les coûts de la collecte initiale

([18]) Recommandation 2003/361/CE du 6 mai 2003 de la Commission concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

des données. Lorsqu'une approbation éthique est nécessaire pour fournir une autorisation de traitement de données, l'évaluation liée à l'approbation éthique devrait être basée sur ses propres mérites.

(70) Les organismes responsables de l'accès aux données de santé devraient être autorisés à percevoir des redevances, en tenant compte des règles horizontales établies par le règlement (UE) 2022/868, en lien avec leurs tâches. Ces redevances pourraient tenir compte de la situation et des intérêts des petites et moyennes entreprises (PME), des chercheurs individuels ou des organismes du secteur public. En particulier, les États membres devraient pouvoir adopter des mesures à l'intention des organismes responsables de l'accès aux données de santé relevant de leur juridiction, permettant d'imposer des redevances réduites à certaines catégories d'utilisateurs de données de santé. Les organismes responsables de l'accès aux données de santé devraient être en mesure de couvrir les coûts de leur fonctionnement au moyen de redevances fixées de manière proportionnée, justifiée et transparente. Cela pourrait entraîner des redevances plus élevées pour certains utilisateurs de données de santé, si la gestion de leurs demandes d'accès aux données de santé et de leurs demandes de données de santé nécessite davantage de travail. Les détenteurs de données de santé devraient être autorisés à demander des redevances pour la mise à disposition des données qui tiennent compte de leurs coûts. Les organismes responsables de l'accès aux données de santé devraient décider du montant de ces redevances, qui pourrait inclure également les redevances demandées par les détenteurs de données de santé. Ces redevances devraient être facturées par l'organisme responsable de l'accès aux données de santé à l'utilisateur de données de santé au moyen d'une facture unique. L'organisme responsable de l'accès aux données de santé devrait ensuite transférer la partie concernée des redevances payées au détenteur de données de santé. Afin de garantir une approche harmonisée concernant les politiques et les structures liées aux redevances, il convient de conférer des compétences d'exécution à la Commission. L'article 10 du règlement (UE) 2023/2854 devrait s'appliquer aux redevances perçues en vertu du présent règlement.

(71) Afin de renforcer l'exécution des règles relatives à l'utilisation secondaire, il convient d'envisager des mesures appropriées pouvant conduire à des amendes administratives ou à des mesures d'exécution de la part des organismes responsables de l'accès aux données de santé ou à des exclusions temporaires ou définitives du cadre de l'EEDS des utilisateurs de données de santé ou des détenteurs de données de santé qui ne respectent pas leurs obligations. Les organismes responsables de l'accès aux données de santé devraient être habilités à vérifier la conformité des utilisateurs de données de santé et des détenteurs de données de santé et devraient leur donner la possibilité de répondre à toute constatation et de remédier à toute violation. Lorsqu'ils statuent sur le montant de l'amende administrative ou sur la mesure d'exécution dans chaque cas individuel, les organismes responsables de l'accès aux données de santé devraient tenir compte des marges de coût et des critères définis dans le présent règlement, pour veiller à ce que ces amendes ou mesures soient proportionnées.

(72) Compte tenu du caractère sensible des données de santé électroniques, il est nécessaire de réduire les risques pour la vie privée des personnes physiques en appliquant le principe de minimisation des données. Par conséquent, les données de santé électroniques à caractère non personnel devraient être mises à disposition dans tous les cas où la fourniture de telles données est suffisante. Si l'utilisateur de données de santé a besoin d'utiliser des données de santé électroniques à caractère personnel, il devrait clairement indiquer dans sa demande la justification de l'utilisation de ce type de données et l'organisme responsable de l'accès aux données de santé devrait évaluer si cette justification est valable. Les données de santé électroniques à caractère personnel ne devraient être mises à disposition que sous un format pseudonymisé. Compte tenu des finalités spécifiques du traitement, les données de santé électroniques à caractère personnel devraient être pseudonymisées ou anonymisées le plus tôt possible dans le processus de mise à disposition des données à des fins d'utilisation secondaire. La pseudonymisation et l'anonymisation devraient pouvoir être effectuées par les organismes responsables de l'accès aux données de santé ou par les détenteurs de données de santé. En tant que responsables du traitement, les organismes responsables de l'accès aux données de santé et les détenteurs de données de santé devraient être autorisés à déléguer ces tâches à des sous-traitants. Lorsqu'il donne accès à un ensemble de données pseudonymisées ou anonymisées, un organisme responsable de l'accès aux données de santé devrait recourir à une technologie et à des normes de pseudonymisation ou d'anonymisation de pointe qui garantissent le plus possible que les personnes physiques ne peuvent pas être réidentifiées par les utilisateurs de données de santé. Il convient de développer davantage cette technologie et ces normes de pseudonymisation ou d'anonymisation des données. Les utilisateurs de données de santé ne devraient pas tenter de réidentifier des personnes physiques à partir de l'ensemble de données fourni au titre du présent règlement, et si c'est le cas, ils devraient se voir imposer les amendes administratives et les mesures d'exécution prévues par le présent règlement, ou des sanctions pénales éventuelles, lorsque le droit national le prévoit. En outre, un demandeur de données de santé devrait pouvoir demander une réponse à une demande de données de santé dans un format statistique anonymisé. Dans ce cas, l'utilisateur de données de santé traitera uniquement des données de santé à caractère non personnel, et l'organisme responsable de l'accès aux données de santé restera le seul responsable du traitement des données à caractère personnel nécessaires pour fournir une réponse à la demande de données de santé.

(73) Afin de garantir que tous les organismes responsables de l'accès aux données de santé délivrent les autorisations de traitement de données de manière similaire, il est nécessaire d'établir une procédure commune standard pour la délivrance des autorisations de traitement de données, avec des demandes similaires dans les différents États membres. Le demandeur de données de santé devrait fournir aux organismes responsables de l'accès aux données de santé plusieurs éléments d'information qui devraient aider l'organisme à évaluer la demande d'accès aux données de santé et à décider si le demandeur de données de santé peut recevoir une autorisation de traitement de données, et la cohérence entre les différents organismes responsables de l'accès aux données de santé devrait être assurée. Les informations fournies dans le cadre de la demande d'accès aux données de santé devraient respecter les exigences établies par le présent règlement afin de permettre son évaluation approfondie, étant donné qu'une autorisation de

traitement de données ne devrait être délivrée que si toutes les conditions nécessaires énoncées dans le présent règlement sont remplies. En outre, le cas échéant, ces informations devraient comprendre une déclaration du demandeur de données de santé selon laquelle l'utilisation prévue des données de santé demandées ne présente pas de risque de stigmatisation ou d'atteinte à la dignité des personnes physiques ou des groupes auxquels se rapporte l'ensemble de données demandé. Une évaluation éthique pourrait être demandée sur la base du droit national. Si tel est le cas, les organismes chargés des questions d'éthique existants devraient pouvoir effectuer ces évaluations pour l'organisme responsable de l'accès aux données de santé. Les organismes chargés des questions d'éthique existants dans les États membres devraient mettre leur expertise à la disposition de l'organisme responsable de l'accès aux données de santé à cette fin. À titre d'alternative, les États membres devraient pouvoir prévoir que les organismes chargés des questions d'éthique font partie de l'organisme responsable de l'accès aux données de santé. L'organisme responsable de l'accès aux données de santé et, le cas échéant, les détenteurs de données de santé, devraient aider les utilisateurs de données de santé à choisir les ensembles de données ou les sources de données qui conviennent à la finalité prévue de l'utilisation secondaire. Lorsque le demandeur de données de santé a besoin de données dans un format statistique anonymisé, il devrait présenter une demande de données de santé, en demandant à l'organisme responsable de l'accès aux données de santé de fournir directement le résultat. Le refus d'une autorisation de traitement de données par l'organisme responsable de l'accès aux données de santé ne devrait pas empêcher le demandeur de données de santé de présenter une nouvelle demande d'accès aux données de santé. Afin de garantir une approche harmonisée entre les organismes responsables de l'accès aux données de santé et de limiter la charge administrative pour les demandeurs de données de santé, la Commission devrait favoriser l'harmonisation des demandes d'accès aux données de santé et des demandes de données de santé, y compris en établissant les modèles pertinents. Dans des cas justifiés, tels qu'une demande complexe et lourde, l'organisme responsable de l'accès aux données de santé devrait être autorisé à prolonger le délai accordé aux détenteurs de données de santé pour mettre les données de santé électroniques demandées à sa disposition.

(74) Étant donné que les ressources des organismes responsables de l'accès aux données de santé sont limitées, ces organismes devraient être autorisés à appliquer des règles de hiérarchisation des priorités, en donnant par exemple la priorité aux institutions publiques par rapport aux entités privées, mais ils ne devraient faire aucune discrimination entre les organismes nationaux et les organismes d'autres États membres au sein de la même catégorie de priorités. L'utilisateur de données de santé devrait pouvoir prolonger la durée de l'autorisation de traitement de données afin, par exemple, de permettre aux réviseurs de publications scientifiques d'accéder aux ensembles de données ou de rendre possible une analyse supplémentaire de l'ensemble de données sur la base des constatations initiales. Cela devrait nécessiter une modification de l'autorisation de traitement de données et pourrait faire l'objet d'une redevance supplémentaire. Cependant, dans tous les cas, l'autorisation de traitement de données devrait refléter ces utilisations supplémentaires de l'ensemble de données. De préférence, l'utilisateur de données de santé devrait les mentionner dans sa demande initiale d'accès aux données de santé. Afin de garantir une approche harmonisée entre les organismes responsables de l'accès aux données de santé, la Commission devrait favoriser l'harmonisation des autorisations de traitement de données.

(75) Comme l'a montré la crise liée à la pandémie de COVID-19, les institutions, organes et organismes de l'Union ayant un mandat légal dans le domaine de la santé publique, en particulier la Commission, ont besoin d'accéder aux données de santé pendant une période plus longue et de manière récurrente. Ce peut être le cas non seulement dans des circonstances spécifiques prévues par le droit de l'Union ou le droit national en temps de crise, mais aussi pour fournir régulièrement des preuves scientifiques et un soutien technique aux politiques de l'Union. L'accès à ces données pourrait être requis dans des États membres spécifiques ou dans l'ensemble du territoire de l'Union. Ces institutions, organes et organismes de l'Union devraient pouvoir bénéficier d'une procédure accélérée pour que les données soient en principe mises à disposition en moins de deux mois, avec la possibilité de prolonger le délai d'un mois dans les cas plus complexes.

(76) Les États membres devraient pouvoir désigner des détenteurs de données de santé de confiance pour lesquels la procédure de délivrance d'une autorisation de traitement de données peut être mise en œuvre de manière simplifiée, afin d'alléger la charge administrative que représente pour les organismes responsables de l'accès aux données de santé la gestion des demandes relatives aux données qu'ils traitent. Les détenteurs de données de santé de confiance devraient être autorisés à évaluer les demandes d'accès aux données de santé présentées dans le cadre de cette procédure simplifiée, sur la base de leur expertise dans le traitement du type de données de santé qu'ils traitent, et de délivrer une recommandation concernant une autorisation de traitement de données. L'organisme responsable de l'accès aux données de santé devrait rester responsable de la délivrance de l'autorisation de traitement de données finale et ne devrait pas être lié par la recommandation fournie par le détenteur de données de santé de confiance. Les entités d'intermédiation de données de santé ne devraient pas être désignées comme détenteurs de données de santé de confiance.

(77) Compte tenu du caractère sensible des données de santé électroniques, les utilisateurs de données de santé ne devraient pas avoir un accès illimité à ces données. Tout accès aux données de santé électroniques demandées à des fins d'utilisation secondaire devrait se faire au moyen d'un environnement de traitement sécurisé. Afin de garantir que des garanties techniques et de sécurité solides sont en place pour les données de santé électroniques, l'organisme responsable de l'accès aux données de santé ou, le cas échéant, le détenteur de données de santé de confiance devrait fournir l'accès à ces données dans un environnement de traitement sécurisé conforme aux normes techniques et de sécurité élevées définies en vertu du présent règlement. Le traitement des données à caractère personnel dans un tel environnement sécurisé devrait être conforme au règlement (UE) 2016/679, y compris, lorsque l'environnement de

traitement sécurisé est géré par un tiers, aux exigences de l'article 28 dudit règlement et, le cas échéant, du chapitre V dudit règlement. Cet environnement de traitement sécurisé devrait réduire les risques pour la vie privée liés à ces activités de traitement et empêcher que les données de santé électroniques soient transmises directement aux utilisateurs de données de santé. L'organisme responsable de l'accès aux données de santé ou le détenteur de données de santé qui fournit ce service devrait garder à tout moment le contrôle sur l'accès aux données de santé électroniques, et l'accès octroyé aux utilisateurs de données de santé devrait être déterminé par les conditions de l'autorisation de traitement de données délivrée. Seules les données de santé électroniques à caractère non personnel qui ne contiennent aucune donnée de santé électronique à caractère personnel devraient être téléchargées par les utilisateurs de données de santé depuis l'environnement de traitement sécurisé. Un tel environnement de traitement sécurisé est donc une garantie essentielle pour préserver les droits et libertés des personnes physiques en ce qui concerne le traitement de leurs données de santé électroniques à des fins d'utilisation secondaire. La Commission devrait aider les États membres à élaborer des normes de sécurité communes afin de promouvoir la sécurité et l'interopérabilité des différents environnements de traitement sécurisés.

(78) Le règlement (UE) 2022/868 fixe les règles générales de gestion de l'altruisme en matière de données. Étant donné que le secteur de la santé gère des données sensibles, des critères supplémentaires devraient être établis au moyen du recueil de règles visé dans ledit règlement. Lorsque ces règles prévoient l'utilisation d'un environnement de traitement sécurisé pour ce secteur, cet environnement de traitement sécurisé devrait respecter les critères établis dans le présent règlement. Les organismes responsables de l'accès aux données de santé devraient coopérer avec les autorités compétentes désignées en vertu du règlement (UE) 2022/868 pour surveiller l'activité des organisations altruistes en matière de données dans le secteur de la santé ou des soins.

(79) Pour le traitement des données de santé électroniques dans le cadre d'une autorisation de traitement de données ou d'une demande de données de santé, les détenteurs de données de santé, y compris les détenteurs de données de santé de confiance, les organismes responsables de l'accès aux données de santé et les utilisateurs de données de santé devraient, chacun à leur tour, être considérés comme les responsables du traitement pour une partie spécifique du processus et en fonction de leurs rôles respectifs dans ce processus. Les détenteurs de données de santé devraient être considérés comme les responsables du traitement pour la divulgation, aux organismes responsables de l'accès aux données de santé, des données de santé électroniques à caractère personnel demandées, tandis que les organismes responsables de l'accès aux données de santé devraient, pour leur part, être considérés comme les responsables du traitement pour le traitement des données de santé électroniques à caractère personnel lors de la préparation des données et de leur mise à la disposition des utilisateurs de données de santé. Les utilisateurs de données de santé devraient être considérés comme les responsables du traitement pour le traitement des données de santé électroniques à caractère personnel dans un format pseudonymisé dans l'environnement de traitement sécurisé en vertu de leurs autorisations de traitement de données. Les organismes responsables de l'accès aux données de santé devraient être considérés comme des sous-traitants pour le compte de l'utilisateur de données de santé pour le traitement effectué par l'utilisateur de données de santé en vertu d'une autorisation de traitement de données dans l'environnement de traitement sécurisé, ainsi que pour le traitement visant à générer une réponse à une demande de données de santé. De la même manière, les détenteurs de données de santé de confiance devraient être considérés comme les responsables du traitement lorsqu'ils traitent des données de santé électroniques à caractère personnel liées à la fourniture de données de santé électroniques à l'utilisateur de données de santé en vertu d'une autorisation de traitement de données ou d'une demande de données de santé. Les détenteurs de données de santé de confiance devraient être considérés comme des sous-traitants pour l'utilisateur de données de santé lorsqu'ils fournissent des données au moyen d'un environnement de traitement sécurisé.

(80) Afin de mettre en place un cadre inclusif et durable pour l'utilisation secondaire plurinationale, une infrastructure transfrontière devrait être établie [DonnéesDeSanté@UE (HealthData@EU)]. DonnéesDeSanté@UE (HealthData@EU) devrait accélérer l'utilisation secondaire tout en renforçant la sécurité juridique, en respectant la vie privée des personnes physiques et en étant interopérable. En raison du caractère sensible des données de santé, des principes tels que le «respect de la vie privée dès la conception» et le «respect de la vie privée par défaut», et le concept de «poser des questions aux données au lieu de déplacer ces données» devraient être respectés chaque fois que cela est possible. Les États membres devraient désigner des points de contact nationaux pour l'utilisation secondaire, en tant que portails organisationnels et techniques pour les organismes responsables de l'accès aux données de santé, et connecter ces points de contact à DonnéesDeSanté@UE (HealthData@EU). Le service d'accès aux données de santé de l'Union devrait également être connecté à DonnéesDeSanté@UE (HealthData@EU). En outre, les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) pourraient être des infrastructures de recherche établies en tant que Consortium pour une infrastructure européenne de recherche (ERIC) en vertu du règlement (CE) n° 723/2009 du Conseil ([19]), en tant que consortium pour une infrastructure numérique européenne (EDIC) au titre de la décision (UE) 2022/2481, ou des infrastructures similaires établies au titre d'autres actes juridiques de l'Union, ainsi que d'autres types d'entités, y compris des infrastructures relevant du forum stratégique européen pour les infrastructures de recherche (ESFRI) ou des infrastructures fédérées dans le cadre du nuage européen pour la science ouverte (EOSC). Les pays tiers et les organisations internationales pourraient également devenir des participants autorisés à DonnéesDeSanté@UE (HealthData@EU), pour autant qu'ils respectent les exigences du présent règlement. La communication du 19 février 2020 de la Commission intitulée «Une stratégie européenne pour les données» a favorisé la mise en relation des différents espaces européens communs des données. DonnéesDeSanté@UE (HealthData@EU) devrait dès lors permettre l'utilisation secondaire de différentes catégories de données de santé électroniques, y compris la mise en relation des données de santé avec des données provenant d'autres espaces de

([19]) Règlement (CE) n° 723/2009 du Conseil du 25 juin 2009 relatif à un cadre juridique communautaire applicable à un Consortium pour une infrastructure européenne de recherche (ERIC) (JO L 206 du 8.8.2009, p. 1).

données tels que ceux relatifs à l'environnement, à l'agriculture et au secteur social. Cette interopérabilité entre le secteur de la santé et d'autres secteurs tels que les secteurs de l'environnement et de l'agriculture et le secteur social pourrait être utile pour obtenir des informations supplémentaires sur les déterminants de la santé. La Commission pourrait fournir un certain nombre de services dans le cadre de DonnéesDeSanté@UE (HealthData@EU), notamment soutenir l'échange d'informations entre les organismes responsables de l'accès aux données de santé et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) pour la gestion des demandes d'accès transfrontière, tenir à jour des catalogues de données de santé électroniques accessibles par l'intermédiaire de l'infrastructure, et fournir des services de découvrabilité du réseau et d'interrogation des métadonnées, de connectivité et de conformité. La Commission pourrait également mettre en place un environnement de traitement sécurisé, permettant la transmission et l'analyse de données provenant de différentes infrastructures nationales, à la demande des responsables du traitement. Dans un souci d'efficacité informatique, de rationalisation et d'interopérabilité des échanges de données, les systèmes existants de partage de données devraient être réutilisés autant que possible, comme ceux en cours de construction pour l'échange de justificatifs dans le cadre du système technique «une fois pour toutes» du règlement (UE) 2018/1724 du Parlement européen et du Conseil ([20]).

(81) En outre, étant donné que la connexion à DonnéesDeSanté@UE (HealthData@EU) pourrait entraîner des transferts de données à caractère personnel liées au demandeur ou à l'utilisateur de données de santé vers des pays tiers, des instruments de transfert pertinents au titre du chapitre V du règlement (UE) 2016/679 doivent être en place pour ces transferts.

(82) Dans le cas de registres ou de bases de données transfrontières, tels que les registres des réseaux européens de référence pour les maladies rares, qui reçoivent des données provenant de différents prestataires de soins de santé dans plusieurs États membres, l'organisme responsable de l'accès aux données de santé de l'État membre où est situé le coordonnateur du registre devrait être chargé de fournir l'accès aux données.

(83) La procédure d'autorisation pour accéder aux données de santé électroniques à caractère personnel dans différents États membres peut être répétitive et lourde pour les utilisateurs de données de santé. Chaque fois que cela est possible, il convient d'établir des synergies afin de réduire la charge et les obstacles pour les utilisateurs de données de santé. L'un des moyens d'atteindre cet objectif consiste à adopter le principe de la «demande unique», selon lequel, avec une seule demande, l'utilisateur de données de santé peut obtenir l'autorisation de plusieurs organismes responsables de l'accès aux données de santé dans différents États membres ou de participants autorisés à DonnéesDeSanté@UE (HealthData@EU).

(84) Les organismes responsables de l'accès aux données de santé devraient fournir des informations sur les ensembles de données disponibles et leurs caractéristiques afin que les utilisateurs de données de santé puissent être informés des faits élémentaires concernant ces ensembles de données et évaluer leur pertinence éventuelle pour eux. C'est pourquoi chaque ensemble de données devrait inclure, au minimum, des informations concernant la source et la nature des données ainsi que les conditions de leur mise à disposition. Le détenteur de données de santé devrait, au moins une fois par an, vérifier que sa description de l'ensemble de données figurant dans le catalogue des ensembles de données national est exacte et à jour. Par conséquent, il convient d'établir un catalogue des ensembles de données de l'UE pour faciliter la découvrabilité des ensembles de données disponibles dans l'EEDS; pour aider les détenteurs de données de santé à publier leurs ensembles de données; pour fournir à toutes les parties prenantes, y compris au grand public, en tenant compte des besoins spécifiques des personnes handicapées, des informations sur les ensembles de données placés dans l'EEDS, telles que les labels de qualité et d'utilité des données et les fiches d'informations relatives aux ensembles de données; et pour fournir aux utilisateurs de données de santé des informations actualisées sur la qualité et l'utilité des données concernant les ensembles de données.

(85) Les informations sur la qualité et l'utilité des ensembles de données augmentent considérablement la valeur des résultats de recherches et d'innovations faisant un usage intensif de données, tout en favorisant, dans le même temps, la prise de décisions réglementaires et politiques fondées sur des données probantes. L'amélioration de la qualité et de l'utilité des ensembles de données grâce au choix éclairé des clients et l'harmonisation des exigences connexes au niveau de l'Union, en tenant compte des normes, des lignes directrices et des recommandations existantes au niveau de l'Union et au niveau international en matière de collecte et d'échange de données, telles que les principes FAIR, profitent également aux détenteurs de données de santé, aux professionnels de la santé, aux personnes physiques et à l'économie de l'Union en général. Un label de qualité et d'utilité des données pour les ensembles de données informerait les utilisateurs de données de santé sur les caractéristiques de qualité et d'utilité d'un ensemble de données et leur permettrait de choisir les ensembles de données qui répondent le mieux à leurs besoins. Le label de qualité et d'utilité des données ne devrait pas empêcher les ensembles de données d'être mis à disposition via l'EEDS, mais devrait offrir un mécanisme de transparence entre les détenteurs de données de santé et les utilisateurs de données de santé. Par exemple, un ensemble de données qui ne répond à aucune exigence en matière de qualité et d'utilité des données devrait porter le label de la catégorie de qualité et d'utilité la plus faible, mais devrait malgré tout être mis à disposition. Les attentes établies par les cadres créés en vertu de l'article 10 du règlement (UE) 2024/1689 et la documentation technique pertinente spécifiée à l'annexe IV dudit règlement devraient être prises en considération lors de l'élaboration du cadre de qualité et d'utilité des données. Les États membres devraient faire connaître le label de qualité et d'utilité des données au moyen d'activités de communication. La Commission pourrait soutenir ces activités. L'utilisation des ensembles de données pourrait être hiérarchisée par leurs utilisateurs en fonction de leur utilité et de leur qualité.

([20]) Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) nº 1024/2012 (JO L 295 du 21.11.2018, p. 1).

(86) Le catalogue des ensembles de données de l'UE devrait réduire au minimum la charge administrative pour les détenteurs de données de santé et les utilisateurs d'autres bases de données, être convivial, accessible et rentable, relier les catalogues des ensembles de données nationaux et éviter l'enregistrement redondant d'ensembles de données. Sans préjudice des exigences énoncées dans le règlement (UE) 2022/868, le catalogue des ensembles de données de l'UE pourrait s'aligner sur l'initiative data.europa.eu. Il convient d'assurer l'interopérabilité entre le catalogue des ensembles de données de l'UE, les catalogues des ensembles de données nationaux et les catalogues des ensembles de données dans les infrastructures de recherche européennes et d'autres infrastructures de partage de données pertinentes.

(87) Des efforts de coopération et des travaux sont en cours entre différentes organisations professionnelles, la Commission et d'autres institutions en vue de définir des champs minimaux de données et d'autres caractéristiques de différents ensembles de données, par exemple, les registres. Ces travaux sont plus avancés dans des domaines tels que le cancer, les maladies rares, les maladies cardiovasculaires et métaboliques, l'évaluation des facteurs de risque et les statistiques, et devraient être pris en considération lors de la définition de nouvelles normes et de modèles harmonisés spécifiques aux maladies pour des éléments de données structurés. Cependant, de nombreux ensembles de données ne sont pas harmonisés, ce qui pose des problèmes de comparabilité et complique la recherche transfrontière. Par conséquent, des règles plus détaillées devraient être définies dans des actes d'exécution afin de garantir l'harmonisation du codage et de l'enregistrement des données de santé électroniques de façon à assurer la cohérence de la fourniture de ces données à des fins d'utilisation secondaire. Ces ensembles de données pourraient comprendre des données provenant des registres des maladies rares, des bases de données sur les médicaments orphelins, des registres des cancers et des registres de maladies infectieuses hautement pertinentes. Les États membres devraient œuvrer en vue d'assurer que les services et les systèmes de santé électroniques européens et les applications interopérables offrent des avantages économiques et sociaux durables, de manière à atteindre un niveau élevé de confiance et de sécurité, à renforcer la continuité des soins de santé et à garantir l'accès à des soins de santé de haute qualité et sûrs. Les infrastructures de données de santé et les registres existants peuvent fournir des modèles utiles pour définir et mettre en œuvre des normes de données et l'interopérabilité, et il convient de les exploiter pour assurer la continuité et tirer parti de l'expertise engrangée.

(88) La Commission devrait aider les États membres à renforcer leurs capacités et leur efficacité dans le domaine des systèmes de santé numérique pour l'utilisation primaire et l'utilisation secondaire. Les États membres devraient être soutenus en vue de renforcer leurs capacités. Les activités menées au niveau de l'Union, telles que les analyses comparatives et l'échange de bonnes pratiques, constituent des mesures pertinentes à cet égard. Ces activités devraient tenir compte des circonstances spécifiques des différentes catégories de parties prenantes, telles que les représentants de la société civile, des chercheurs, des sociétés médicales et des PME.

(89) L'amélioration de la maîtrise des outils de santé numérique, tant pour les personnes physiques que pour les professionnels de la santé, est essentielle pour instaurer la confiance et la sécurité et pour utiliser correctement les données de santé, et est donc essentielle pour parvenir à mettre pleinement en œuvre le présent règlement. Les professionnels de la santé font face à de profonds changements dans le contexte de la numérisation et se verront encore proposer d'autres outils numériques dans le cadre de la mise en œuvre de l'EEDS. En conséquence, les professionnels de la santé doivent développer leur maîtrise des outils de santé numérique et leurs compétences numériques et les États membres devraient fournir aux professionnels de la santé l'accès à des cours d'utilisation des outils numériques afin de pouvoir se préparer à travailler avec des systèmes de DME. Ces cours devraient permettre aux professionnels de la santé et aux techniciens informatiques d'être suffisamment formés pour travailler avec de nouvelles infrastructures numériques pour garantir la cybersécurité et la gestion éthique des données de santé. Les cours de formation devraient être élaborés, révisés et tenus à jour régulièrement, en concertation et en coopération avec les experts concernés. L'amélioration de la maîtrise des outils de santé numérique est cruciale pour permettre aux personnes physiques d'exercer un véritable contrôle sur leurs données de santé, de gérer de manière active leur santé et les soins en ce qui les concerne, et de comprendre les implications de la gestion de ces données tant à des fins d'utilisation primaire que d'utilisation secondaire. Les divers groupes démographiques présentent des niveaux variables de maîtrise des outils numériques, ce qui peut entraver la capacité des personnes physiques à exercer leurs droits de contrôler leurs données de santé électroniques. Il convient donc que les États membres, collectivités régionales et locales comprises, soutiennent la maîtrise des outils de santé numérique et la sensibilisation du public, tout en s'assurant que la mise en œuvre du présent règlement contribue à la réduction des inégalités et n'entraîne pas de discrimination à l'encontre des populations présentant des lacunes en matière de compétences numériques. Une attention particulière devrait être portée aux personnes handicapées et aux groupes vulnérables, dont les migrants et les personnes âgées. Les États membres devraient créer des programmes nationaux ciblés de maîtrise des outils numériques, y compris des programmes visant à maximiser l'inclusion sociale et à garantir que toutes les personnes physiques peuvent effectivement exercer les droits que leur confère le présent règlement. Les États membres devraient également fournir aux personnes physiques des orientations centrées sur le patient en ce qui concerne l'utilisation des dossiers médicaux électroniques et l'utilisation primaire de leurs données de santé électroniques à caractère personnel. Les orientations devraient être adaptées au niveau de maîtrise des outils de santé numérique du patient, en accordant une attention particulière aux besoins des groupes vulnérables.

(90) L'utilisation de fonds devrait également contribuer à atteindre les objectifs de l'EEDS. Les acheteurs publics, les autorités nationales compétentes des États membres, y compris les autorités de santé numérique et les organismes responsables de l'accès aux données de santé, ainsi que la Commission devraient faire référence aux spécifications techniques, normes et profils applicables en matière d'interopérabilité, de sécurité et de qualité des données, ainsi qu'aux autres exigences élaborées au titre du présent règlement, lorsqu'ils définissent les conditions des marchés

publics, des appels à propositions et de l'attribution des fonds de l'Union, y compris les Fonds structurels et de cohésion. Les fonds de l'Union doivent être répartis de manière transparente entre les États membres, en tenant compte des différents niveaux de numérisation des systèmes de santé. La mise à disposition de données à des fins d'utilisation secondaire nécessite des ressources supplémentaires pour les systèmes de soins de santé, en particulier les systèmes de soins de santé publics. Il convient d'aborder cette question et de réduire au minimum cette charge supplémentaire pendant la phase de mise en œuvre de l'EEDS.

(91) La mise en œuvre de l'EEDS nécessite des investissements appropriés dans le renforcement des capacités et la formation, ainsi qu'un bon engagement financier en faveur de la consultation et de la participation du public au niveau de l'Union et au niveau national. Les coûts économiques de la mise en œuvre du présent règlement devront être supportés tant au niveau de l'Union qu'au niveau national, et il faudra parvenir à un partage équitable de cette charge entre les fonds de l'Union et les fonds nationaux.

(92) Certaines catégories de données de santé électroniques peuvent rester particulièrement sensibles même lorsqu'elles sont anonymisées et donc à caractère non personnel, comme le prévoit déjà spécifiquement le règlement (UE) 2022/868. Même en cas d'utilisation de techniques d'anonymisation de pointe, il subsiste un risque résiduel que la capacité de réidentification soit ou devienne disponible, au-delà des moyens raisonnablement susceptibles d'être utilisés. Ce risque résiduel est présent en ce qui concerne les maladies rares, c'est-à-dire des affections entraînant une menace pour la vie ou une invalidité chronique ne touchant pas plus de cinq personnes sur dix mille dans l'Union, pour lesquelles le nombre limité de cas réduit la possibilité d'agréger intégralement les données publiées afin de préserver la vie privée des personnes physiques tout en maintenant un niveau de granularité approprié afin de rester significatif. Ce risque résiduel peut avoir une incidence sur différentes catégories de données de santé et peut conduire à la réidentification des personnes concernées à l'aide de moyens qui vont au-delà de ceux qui sont raisonnablement susceptibles d'être utilisés. Ce risque dépend du niveau de granularité, de la description des caractéristiques des personnes concernées, du nombre de personnes touchées, par exemple, dans le cas de données figurant dans les dossiers médicaux électroniques, les registres de maladies, les biobanques et les données générées par les personnes, lorsque l'éventail des caractéristiques d'identification est plus large, et de la combinaison possible avec d'autres informations, par exemple dans des zones géographiques très limitées, ou en raison de l'évolution technologique de méthodes qui n'étaient pas disponibles au moment de l'anonymisation. Une telle réidentification de personnes physiques susciterait une préoccupation majeure et risquerait de compromettre l'acceptation des règles relatives à l'utilisation secondaire prévues par le présent règlement. En outre, les techniques d'agrégation sont moins éprouvées pour les données à caractère non personnel contenant par exemple des secrets d'affaires, comme dans le cadre de la notification d'essais cliniques et d'investigations cliniques, et, en l'absence d'une norme internationale de protection suffisante, il est plus difficile de réprimer les violations des secrets d'affaires en dehors de l'Union. Par conséquent, pour ces catégories de données de santé, il subsiste un risque de réidentification après l'anonymisation ou l'agrégation, qui ne peut pas être raisonnablement atténué au départ. Cela relève des critères énoncés à l'article 5, paragraphe 13, du règlement (UE) 2022/868. Ces types de données de santé relèveraient donc de l'habilitation prévue à l'article 5, paragraphe 13, dudit règlement pour le transfert vers des pays tiers. Les conditions particulières prévues dans le cadre de l'habilitation énoncée à l'article 5, paragraphe 13, du règlement (UE) 2022/868 seront détaillées dans le cadre de l'acte délégué adopté au titre de cette habilitation, et doivent être proportionnées au risque de réidentification et tenir compte des spécificités des différentes catégories de données ou des différentes techniques d'anonymisation ou d'agrégation.

(93) Le traitement de grandes quantités de données de santé électroniques à caractère personnel aux fins de l'EEDS, lors d'activités de traitement de données dans le cadre de la gestion des demandes d'accès aux données de santé, des autorisations de traitement de données et des demandes de données de santé, comporte des risques plus élevés d'accès non autorisé à ces données à caractère personnel, ainsi que la possibilité d'incidents de cybersécurité. Les données de santé électroniques à caractère personnel sont particulièrement sensibles, car elles contiennent souvent des informations couvertes par le secret médical, dont la divulgation à des tiers non autorisés peut causer des difficultés importantes. En tenant pleinement compte des principes énoncés dans la jurisprudence de la Cour de justice de l'Union européenne, le présent règlement garantit le plein respect des droits fondamentaux, du droit au respect de la vie privée et du principe de proportionnalité. Afin d'assurer la pleine intégrité et la confidentialité des données de santé électroniques à caractère personnel au titre du présent règlement, de garantir un niveau particulièrement élevé de protection et de sécurité et de réduire le risque d'accès illicite à ces données de santé électroniques à caractère personnel, le présent règlement permet aux États membres d'exiger que les données de santé électroniques à caractère personnel soient conservées et traitées uniquement au sein de l'Union aux fins de l'exécution des tâches prévues par le présent règlement, à moins qu'une décision d'adéquation adoptée en vertu de l'article 45 du règlement (UE) 2016/679 ne s'applique.

(94) L'accès aux données de santé électroniques pour les utilisateurs de données de santé établis dans des pays tiers ou pour des organisations internationales ne devrait avoir lieu que sur la base du principe de réciprocité. La mise à la disposition d'un pays tiers de données de santé électroniques ne devrait pouvoir avoir lieu que lorsque la Commission a établi, par voie d'un acte d'exécution, que le pays tiers concerné permet aux entités de l'Union d'accéder aux données de santé électroniques en provenance de ce pays tiers dans les mêmes conditions et avec les mêmes garanties que s'ils accédaient à des données de santé électroniques au sein de l'Union. La Commission devrait

suivre et réexaminer à intervalles réguliers la situation dans ces pays tiers et à l'égard des organisations internationales, et dresser une liste de ces actes d'exécution. Lorsque la Commission constate qu'un pays tiers n'assure plus l'accès aux mêmes conditions, elle devrait abroger l'acte d'exécution correspondant.

(95) Afin de promouvoir l'application cohérente du présent règlement, y compris en ce qui concerne l'interopérabilité transfrontière des données de santé électroniques, un comité de l'espace européen des données de santé devrait être institué. La Commission devrait participer à ses activités et le coprésider. Le comité de l'EEDS devrait pouvoir fournir des contributions écrites liées à l'application cohérente du présent règlement dans l'ensemble de l'Union, notamment en aidant les États membres à coordonner l'utilisation des données de santé électroniques pour les soins de santé et la certification, mais aussi concernant l'utilisation secondaire et le financement de ces activités. Cela pourrait également inclure le partage d'informations sur les risques et les incidents dans les environnements de traitement sécurisés. Le partage de ce type d'informations n'affecte pas les obligations prévues dans d'autres actes juridiques, telles que les notifications de violations de données au titre du règlement (UE) 2016/679. Plus généralement, les activités du comité de l'EEDS sont sans préjudice des pouvoirs des autorités de contrôle en vertu du règlement (UE) 2016/679. Étant donné que, au niveau national, les autorités de santé numérique qui s'occupent de l'utilisation primaire peuvent être différentes des organismes responsables de l'accès aux données de santé qui s'occupent de l'utilisation secondaire, que ces fonctions sont différentes et qu'il est nécessaire de coopérer de manière distincte dans chacun de ces domaines, le comité de l'EEDS devrait pouvoir créer des sous-groupes chargés de ces deux fonctions, ainsi que d'autres sous-groupes, selon les besoins. Pour travailler de manière efficace, les autorités de santé numérique et les organismes responsables de l'accès aux données de santé devraient créer des réseaux et des liens au niveau national avec d'autres organismes et autorités, mais aussi au niveau de l'Union. Ces organismes pourraient comprendre les autorités chargées de la protection des données, les organismes de cybersécurité, d'identification électronique et de normalisation, ainsi que les organismes et groupes d'experts relevant des règlements (UE) 2022/868, (UE) 2023/2854 et (UE) 2024/1689 et du règlement (UE) 2019/881 du Parlement européen et du Conseil ([21]). Le comité de l'EEDS devrait fonctionner de manière indépendante, dans l'intérêt public et conformément à son code de conduite.

(96) Lorsque des questions considérées par le comité de l'EEDS comme présentant un intérêt particulier sont examinées, le comité de l'EEDS devrait pouvoir inviter des observateurs, par exemple le CEPD, des représentants des institutions de l'Union, y compris du Parlement européen, et d'autres parties prenantes.

(97) Un forum des parties prenantes devrait être mis en place pour conseiller le comité de l'EEDS dans l'accomplissement de ses tâches en apportant la contribution des parties prenantes sur les questions relatives au présent règlement. Le forum des parties prenantes devrait être composé, entre autres, de représentants des organisations de patients et de consommateurs, des professionnels de la santé, des entreprises, des chercheurs scientifiques et du monde universitaire. Sa composition devrait être équilibrée et il devrait représenter les points de vue des différentes parties prenantes concernées. Les intérêts tant commerciaux que non commerciaux devraient être représentés.

(98) Afin d'assurer la bonne gestion courante des infrastructures transfrontières pour l'utilisation primaire et l'utilisation secondaire, il est nécessaire de créer des groupes de pilotage composés de représentants des États membres. Ces groupes de pilotage devraient prendre les décisions opérationnelles concernant la gestion technique courante des infrastructures transfrontières et leur développement technique, y compris en ce qui concerne les modifications techniques apportées aux infrastructures, l'amélioration des fonctionnalités ou des services, ou la garantie de l'interopérabilité avec d'autres infrastructures, systèmes numériques ou espaces de données. Leurs activités ne devraient pas comprendre la contribution à l'élaboration d'actes d'exécution concernant ces infrastructures. Ces groupes de pilotage devraient pouvoir également inviter des représentants d'autres participants autorisés à DonnéesDeSanté@UE (HealthData@EU) en tant qu'observateurs à leurs réunions et devraient consulter les experts compétents dans l'accomplissement de leurs tâches.

(99) Sans préjudice de tout autre recours administratif, judiciaire ou extrajudiciaire, toute personne physique ou morale qui estime que ses droits ou intérêts au titre du présent règlement ont été lésés devrait avoir le droit d'introduire une réclamation auprès d'une autorité de santé numérique ou d'un organisme responsable de l'accès aux données de santé. L'enquête faisant suite à une réclamation devrait être menée, sous réserve d'un contrôle juridictionnel, dans la mesure appropriée au cas d'espèce. L'autorité de santé numérique ou l'organisme responsable de l'accès aux données de santé devrait informer la personne physique ou morale de l'état d'avancement et de l'issue de la réclamation dans un délai raisonnable. Si l'affaire nécessite un complément d'enquête ou une coordination avec une autre autorité de santé numérique ou un autre organisme responsable de l'accès aux données de santé, des informations sur les progrès réalisés dans le traitement de la réclamation devraient être fournies à la personne physique ou morale. Afin de faciliter l'introduction des réclamations, chaque autorité de santé numérique et chaque organisme responsable de l'accès aux données de santé devraient prendre des mesures telles que la fourniture d'un formulaire d'introduction de

([21]) Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

réclamation pouvant également être rempli par voie électronique, sans exclure la possibilité d'utiliser d'autres moyens de communication. Lorsque la réclamation concerne les droits de personnes physiques liés à la protection de leurs données à caractère personnel, l'autorité de santé numérique ou l'organisme responsable de l'accès aux données devrait transmettre la réclamation aux autorités de contrôle au titre du règlement (UE) 2016/679. Les autorités de santé numérique ou les organismes responsables de l'accès aux données de santé devraient coopérer pour traiter les réclamations et y apporter une réponse, y compris en échangeant toutes les informations pertinentes par voie électronique, dans les meilleurs délais.

(100) Lorsqu'une personne physique estime que les droits que lui confère le présent règlement ont été violés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association à but non lucratif, constitués conformément au droit national, dont les objectifs statutaires sont d'intérêt public et qui sont actifs dans le domaine de la protection des données à caractère personnel, pour qu'ils introduisent une réclamation en son nom.

(101) L'autorité de santé numérique, l'organisme responsable de l'accès aux données de santé, le détenteur de données de santé ou l'utilisateur de données de santé devraient indemniser tout dommage qu'une personne physique ou morale subit du fait d'une violation du présent règlement. La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice de l'Union européenne, d'une manière qui tienne pleinement compte des objectifs du présent règlement. Cela est sans préjudice de toute demande d'indemnisation pour un dommage découlant de la violation d'autres dispositions du droit de l'Union ou du droit national. Les personnes physiques devraient obtenir une réparation complète et effective pour le dommage subi.

(102) Afin de renforcer l'exécution des règles du présent règlement, des sanctions, y compris des amendes administratives, devraient être imposées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par les organismes responsables de l'accès aux données de santé en vertu du présent règlement. L'imposition de sanctions, y compris d'amendes administratives, devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

(103) Il convient de prévoir des dispositions permettant aux organismes responsables de l'accès aux données de santé d'appliquer des amendes administratives pour certaines violations du présent règlement qui devraient être considérées comme des violations graves, telles que la réidentification de personnes physiques, le téléchargement de données de santé électroniques à caractère personnel en dehors de l'environnement de traitement sécurisé ou le traitement de données à des fins d'utilisations interdites ou d'utilisations non couvertes par une autorisation de traitement de données. Le présent règlement devrait définir ces violations ainsi que le montant maximal et les critères de fixation des amendes administratives y afférentes, qui devraient être fixés par l'organisme responsable de l'accès aux données de santé compétent dans chaque cas d'espèce, en prenant en considération toutes les circonstances pertinentes propres à chaque cas et compte dûment tenu, notamment, de la nature, de la gravité et de la durée de la violation et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations prévues au présent règlement et pour prévenir ou atténuer les conséquences de la violation. Aux fins de l'imposition d'amendes administratives au titre du présent règlement, le concept d'«entreprise» devrait être compris conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. Le fait d'imposer une amende administrative ou le fait de donner un avertissement ne devrait pas porter atteinte à l'exercice d'autres pouvoirs des organismes responsables de l'accès aux données de santé ou à l'application d'autres sanctions au titre du présent règlement.

(104) Pour garantir que l'EEDS atteigne ses objectifs, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne la modification ou l'ajout dans l'annexe I ou le retrait de ladite annexe des principales caractéristiques des catégories prioritaires des données de santé électroniques à caractère personnel, la liste des données requises à introduire par les fabricants de systèmes de DME et d'applications de bien-être dans la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être ainsi que la modification, l'ajout ou le retrait d'éléments destinés à être couverts par le label de qualité et d'utilité des données. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer» ([22]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(105) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne:

— les spécifications techniques pour l'interopérabilité des services de procuration des États membres,

([22]) JO L 123 du 12.5.2016, p. 1.

— les exigences en matière de qualité des données pour l'enregistrement des données de santé électroniques à caractère personnel dans un système de DME,

— les spécifications transfrontières pour les catégories prioritaires de données de santé électroniques à caractère personnel,

— les spécifications techniques pour les catégories de données de santé électroniques à caractère personnel, fixant le format européen d'échange des dossiers médicaux électroniques,

— les mises à jour du format européen d'échange des dossiers médicaux électroniques pour intégrer les révisions pertinentes des systèmes de codage et les nomenclatures des soins de santé,

— les spécifications techniques pour étendre le format européen d'échange des dossiers médicaux électroniques à des catégories de données de santé électroniques à caractère personnel supplémentaires,

— les exigences applicables au mécanisme interopérable et transfrontière d'identification et d'authentification pour les personnes physiques et les professionnels de la santé, conformément au règlement (UE) n° 910/2014,

— les exigences applicables à la mise en œuvre technique des droits des personnes physiques en ce qui concerne l'utilisation primaire de leurs données de santé électroniques à caractère personnel,

— les mesures nécessaires au développement technique de MaSanté@UE (MyHealth@EU), les règles détaillées concernant la sécurité, la confidentialité et la protection des données de santé électroniques à caractère personnel et les conditions applicables aux contrôles de conformité nécessaires pour adhérer et rester connecté à MaSanté@UE (MyHealth@EU),

— les règles concernant les exigences en matière de cybersécurité, d'interopérabilité technique, d'interopérabilité sémantique, d'opérations et de gestion des services en ce qui concerne le traitement par la Commission et ses responsabilités à l'égard des responsables du traitement,

— les aspects techniques des services supplémentaires fournis par l'intermédiaire de MaSanté@UE (MyHealth@EU),

— les aspects techniques des échanges de données de santé électroniques à caractère personnel entre MaSanté@UE MyHealth@EU) et d'autres services ou infrastructures,

— la connexion d'autres infrastructures, de points de contact nationaux pour la santé numérique de pays tiers ou de systèmes établis à l'échelon international par des organisations internationales à la plateforme d'interopérabilité centrale de MaSanté@UE (MyHealth@EU) et la déconnexion de ceux-ci de ladite plateforme,

— les spécifications communes en ce qui concerne les exigences essentielles fixées à l'annexe II,

— les spécifications communes applicables à l'environnement d'essai numérique européen,

— les justifications des mesures nationales prises par les autorités de surveillance du marché en cas de non-conformité des systèmes de DME,

— le format et le contenu du label des applications de bien-être,

— les principes applicables aux politiques et aux structures liées aux redevances en ce qui concerne les redevances que les organismes responsables de l'accès aux données de santé et les détenteurs de données de santé de confiance peuvent facturer pour la mise à disposition de données de santé électroniques à des fins d'utilisation secondaire,

— l'architecture d'un outil informatique destiné à soutenir les mesures d'exécution et à les rendre transparentes pour les organismes responsables de l'accès aux données de santé,

— le logo permettant de reconnaître la contribution de l'EDHS,

— les modèles pour la demande d'accès aux données de santé, pour l'autorisation de traitement de données et pour la demande de données de santé,

— les exigences techniques et organisationnelles, ainsi que les exigences en matière de sécurité de l'information, de confidentialité, de protection des données et d'interopérabilité applicables aux environnements de traitement sécurisés,

— les modèles pour les accords entre les responsables du traitement et les sous-traitants,

— les décisions portant sur le respect, par un point de contact national pour l'utilisation secondaire d'un pays tiers ou un système établi à l'échelon international par des organisations internationales, des exigences de DonnéesDeSanté@UE (HealthData@EU) aux fins de l'utilisation secondaire des données de santé, sur le respect du chapitre IV et sur la question de savoir si ce point de contact national pour l'utilisation secondaire ou ce système donne aux utilisateurs de données de santé situés dans l'Union un accès équivalent aux données de santé électroniques auxquelles il a accès,

— les exigences, les spécifications techniques et l'architecture informatique de DonnéesDeSanté@UE (HealthData@EU); les conditions et les contrôles de conformité pour adhérer et rester connecté à DonnéesDeSanté@UE (HealthData@EU); les critères minimaux que doivent remplir les points de contact nationaux pour l'utilisation secondaire et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU); les responsabilités des responsables du traitement et des sous-traitants participant à DonnéesDeSanté@UE (HealthData@EU); les responsabilités des responsables du traitement et des sous-traitants en ce qui concerne l'environnement de traitement sécurisé géré par la Commission; et les spécifications communes applicables à l'architecture de DonnéesDeSanté@UE (HealthData@EU) et à son interopérabilité avec d'autres espaces européens communs des données,

— les décisions visant à connecter des participants autorisés individuels à DonnéesDeSanté@UE (HealthData@EU),

— les éléments minimaux pour les ensembles de données et les caractéristiques de ces éléments à fournir par les détenteurs de données de santé,

— les caractéristiques visuelles et les spécifications techniques du label de qualité et d'utilité des données,

— les spécifications minimales applicables aux ensembles de données ayant une incidence majeure sur l'utilisation secondaire,

— les décisions portant sur la question de savoir si un pays tiers permet aux demandeurs de données de santé de l'Union d'accéder aux données de santé électroniques dans ledit pays tiers à des conditions qui ne sont pas plus restrictives que celles prévues dans le présent règlement,

— les mesures nécessaires à la création et au fonctionnement du comité de l'EEDS.

Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([23]).

(106) Les États membres devraient prendre toutes les mesures nécessaires pour garantir que les dispositions du présent règlement sont mises en œuvre, notamment en prévoyant des sanctions effectives, proportionnées et dissuasives en cas de violation de ces dispositions. Pour décider du montant de la sanction dans chaque cas d'espèce, les États membres devraient tenir compte des limites et des critères définis dans le présent règlement. La réidentification de personnes physiques devrait être considérée comme une violation grave du présent règlement.

(107) La mise en œuvre de l'EEDS nécessitera d'importants travaux de développement dans les États membres et les services centraux. Pour suivre les progrès accomplis à cet égard, la Commission devrait élaborer des rapports annuels sur ces progrès, jusqu'à la pleine application du présent règlement, en tenant compte des informations fournies par les États membres. Ces rapports pourraient comprendre des recommandations de mesures correctives, ainsi qu'une évaluation des progrès accomplis.

(108) Afin de déterminer si le présent règlement atteint ses objectifs de manière effective et efficace, s'il est cohérent et toujours pertinent et s'il apporte une valeur ajoutée au niveau de l'Union, la Commission devrait procéder à une évaluation du présent règlement. La Commission devrait procéder à une évaluation ciblée du présent règlement au plus tard huit ans à compter de son entrée en vigueur, et à une évaluation globale du présent règlement au plus tard dix ans à compter de son entrée en vigueur. La Commission devrait présenter des rapports sur ses principales constatations à la suite de chaque évaluation au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions.

(109) Pour une mise en œuvre transfrontière réussie de l'EEDS, le cadre d'interopérabilité européen, dont le champ d'application a été mis à jour et étendu par la communication de la Commission du 23 mars 2017 intitulée «Cadre d'interopérabilité européen — Stratégie de mise en œuvre» en vue d'intégrer de nouvelles exigences ou des exigences revues en matières d'interopérabilité, devrait être considéré comme une référence commune pour garantir l'interopérabilité juridique, organisationnelle, sémantique et technique.

(110) Étant donné que les objectifs du présent règlement, à savoir autonomiser les personnes physiques en leur permettant d'exercer un contrôle accru sur leurs données de santé électroniques à caractère personnel et en favorisant la libre circulation des personnes physiques en garantissant que leurs données de santé les suivent; favoriser un véritable marché intérieur des services et produits de santé numérique et garantir un cadre cohérent et efficace pour la réutilisation des données de santé des personnes physiques à des fins de recherche, d'innovation, d'élaboration de politiques et d'activités réglementaires, ne peuvent pas être atteints de manière suffisante par les États membres

([23]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

uniquement au moyen de mesures de coordination, comme l'a montré l'évaluation des aspects numériques de la directive 2011/24/UE, mais peuvent, en raison de mesures d'harmonisation relatives aux droits des personnes physiques en ce qui concerne leurs données de santé électroniques, à l'interopérabilité des données de santé électroniques et à un cadre et des garanties communs pour l'utilisation primaire et l'utilisation secondaire, être mieux atteints au niveau de l'Union, l'Union peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(111) Il ressort de l'évaluation des aspects numériques de la directive 2011/24/UE que l'efficacité du réseau «Santé en ligne» est limitée, mais aussi qu'il existe un fort potentiel de travail à l'échelon de l'Union dans le domaine de la santé numérique, comme l'a montré le travail effectué pendant la pandémie de COVID-19. La directive 2011/24/UE devrait dès lors être modifiée en conséquence.

(112) Le présent règlement complète les exigences essentielles en matière de cybersécurité énoncées dans le règlement (UE) 2024/2847. Les systèmes de DME qui sont des produits comportant des éléments numériques au sens du règlement (UE) 2024/2847 devraient dès lors respecter les exigences essentielles en matière de cybersécurité énoncées dans ledit règlement. Les fabricants de ces systèmes de DME devraient apporter la preuve de leur conformité comme l'exige le présent règlement. Pour faciliter cette conformité, les fabricants devraient pouvoir établir une seule documentation technique contenant les éléments requis par les deux actes juridiques. Il devrait être possible de démontrer la conformité des systèmes de DME aux exigences essentielles en matière de cybersécurité énoncées dans le règlement (UE) 2024/2847 au moyen du cadre d'évaluation prévu par le présent règlement. Cependant, les parties de la procédure d'évaluation de la conformité prévue par le présent règlement qui se rapportent à l'utilisation d'environnements d'essai ne devraient pas s'appliquer, puisque ces environnements d'essai ne permettent pas une évaluation de la conformité aux exigences essentielles en matière de cybersécurité. Comme le règlement (UE) 2024/2847 ne couvre pas directement les logiciels service (SaaS) en tant que tels, les systèmes de DME offerts via le modèle de licence et de distribution SaaS ne relèvent pas du champ d'application dudit règlement. De la même manière, les systèmes de DME qui sont développés en interne ne relèvent pas du champ d'application dudit règlement, puisqu'ils ne sont pas placés sur le marché.

(113) Le CEPD et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis conjoint le 12 juillet 2022.

(114) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles de concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne.

(115) Compte tenu de la nécessité d'une préparation technique, le présent règlement devrait être applicable à compter du 26 mars 2027. Afin de favoriser la mise en œuvre réussie de l'EEDS et la création de conditions efficaces pour la coopération européenne en matière de données de santé, la mise en œuvre devrait avoir lieu par étapes,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. Le présent règlement établit l'espace européen des données de santé (EEDS) en prévoyant des règles, des normes et des infrastructures communes et un cadre de gouvernance, en vue de faciliter l'accès aux données de santé électroniques aux fins de l'utilisation primaire des données de santé électroniques et de l'utilisation secondaire de ces données.

2. Le présent règlement:

a) précise et complète les droits des personnes physiques en ce qui concerne l'utilisation primaire et l'utilisation secondaire de leurs données de santé électroniques à caractère personnel fixés par le règlement (UE) 2016/679;

b) établit des règles communes pour les systèmes de dossiers médicaux électroniques (ci-après dénommés «systèmes de DME») en ce qui concerne deux composants logiciels harmonisés obligatoires, à savoir le composant logiciel d'interopérabilité européen pour les systèmes de DME et le composant logiciel de journalisation européen pour les systèmes de DME, tels qu'ils sont définis, respectivement, à l'article 2, paragraphe 2, points n) et o), et pour les

applications de bien-être au sujet desquelles l'interopérabilité avec les systèmes de DME en ce qui concerne ces deux composants logiciels harmonisés est alléguée, en ce qui concerne l'utilisation primaire des données de santé électroniques;

c) établit des règles et des mécanismes communs pour l'utilisation primaire des données de santé électroniques et l'utilisation secondaire des données de santé électroniques;

d) met en place une infrastructure transfrontière permettant l'utilisation primaire des données de santé électroniques à caractère personnel dans l'ensemble de l'Union;

e) met en place une infrastructure transfrontière pour l'utilisation secondaire des données de santé électroniques;

f) établit des mécanismes de gouvernance et de coordination au niveau de l'Union et au niveau national à la fois pour l'utilisation primaire des données de santé électroniques et l'utilisation secondaire des données de santé électroniques.

3. Le présent règlement s'entend sans préjudice d'autres actes juridiques de l'Union concernant l'accès aux données de santé électroniques, ainsi que leur partage ou leur utilisation secondaire, ou des exigences de l'Union concernant le traitement de données en ce qui concerne les données de santé électroniques, en particulier des règlements (CE) nº 223/2009 ([24]), (UE) nº 536/2014 ([25]), (UE) 2016/679, (UE) 2018/1725, (UE) 2022/868 et (UE) 2023/2854 du Parlement européen et du Conseil, et des directives 2002/58/CE ([26]) et (UE) 2016/943 ([27]) du Parlement européen et du Conseil.

4. Les références faites dans le présent règlement aux dispositions du règlement (UE) 2016/679 s'entendent également comme des références faites aux dispositions correspondantes du règlement (UE) 2018/1725, le cas échéant, en ce qui concerne les institutions, organes et organismes de l'Union.

5. Le présent règlement s'entend sans préjudice des règlements (UE) 2017/745, (UE) 2017/746 et (UE) 2024/1689, en ce qui concerne la sécurité des dispositifs médicaux, des dispositifs médicaux de diagnostic in vitro et des systèmes d'intelligence artificielle (IA) qui interagissent avec les systèmes de DME.

6. Le présent règlement s'entend sans préjudice du droit de l'Union ou du droit national relatif au traitement des données de santé électroniques aux fins de la notification, de la réponse aux demandes d'accès à des informations ou de la démonstration ou vérification du respect des obligations légales, ou du droit de l'Union ou du droit national en ce qui concerne l'octroi de l'accès aux documents officiels et leur divulgation.

7. Le présent règlement s'entend sans préjudice des dispositions spécifiques du droit de l'Union ou du droit national prévoyant l'accès aux données de santé électroniques en vue d'un traitement ultérieur par les organismes du secteur public des États membres, par les institutions, organes et organismes de l'Union ou par des entités privées chargées, en vertu du droit de l'Union ou du droit national, d'une mission d'intérêt public, aux fins de l'accomplissement de cette mission.

8. Le présent règlement n'a pas d'incidence sur l'accès aux données de santé électroniques à des fins d'utilisation secondaire convenu dans le cadre d'accords contractuels ou administratifs entre entités publiques ou privées.

9. Le présent règlement ne s'applique pas au traitement de données à caractère personnel dans les cas suivants:

a) lorsque le traitement est effectué au cours d'une activité qui ne relève pas du champ d'application du droit de l'Union;

b) lorsque le traitement est effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris à des fins de protection contre des menaces pour la sécurité publique et de prévention de telles menaces.

([24]) Règlement (CE) nº 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) nº 1101/2008 du Parlement européen et du Conseil relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) nº 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).

([25]) Règlement (UE) nº 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE (JO L 158 du 27.5.2014, p. 1).

([26]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (JO L 201 du 31.7.2002, p. 37).

([27]) Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

Article 2

Définitions

1. Aux fins du présent règlement, les définitions suivantes s'appliquent:

a) les définitions des termes «données à caractère personnel», «traitement», «pseudonymisation», «responsable du traitement», «sous-traitant», «tiers», «consentement», «données génétiques», «données concernant la santé» et «organisation internationale» figurant à l'article 4, points 1), 2), 5), 7), 8), 10), 11), 13), 15) et 26), respectivement, du règlement (UE) 2016/679;

b) les définitions des termes «soins de santé», «État membre d'affiliation», «État membre de traitement», «professionnel de la santé», «prestataire de soins de santé», «médicament» et «prescription» figurant à l'article 3, points a), c), d), f), g), i) et k), respectivement, de la directive 2011/24/UE;

c) les définitions des termes «données», «accès», «altruisme en matière de données», «organisme du secteur public» et «environnement de traitement sécurisé» figurant à l'article 2, points 1), 13), 16), 17) et 20), respectivement, du règlement (UE) 2022/868;

d) les définitions des termes «mise à disposition sur le marché», «mise sur le marché», «surveillance du marché», «autorité de surveillance du marché», «non-conformité», «fabricant», «importateur», «distributeur», «opérateur économique», «mesure corrective», «rappel» et «retrait» figurant à l'article 3, points 1), 2), 3), 4), 7), 8), 9), 10), 13), 16), 22) et 23), respectivement, du règlement (UE) 2019/1020;

e) les définitions des termes «dispositif médical», «destination», «notice d'utilisation», «performances», «établissement de santé» et «spécifications communes» figurant à l'article 2, points 1), 12), 14), 22), 36) et 71), respectivement, du règlement (UE) 2017/745;

f) les définitions des termes «identification électronique» et «moyen d'identification électronique» figurant à l'article 3, points 1) et 2), respectivement, du règlement (UE) nº 910/2014;

g) la définition de «pouvoirs adjudicateurs» figurant à l'article 2, paragraphe 1, point 1), de la directive 2014/24/UE du Parlement européen et du Conseil ([28]);

h) la définition de «santé publique» figurant à l'article 3, point c), du règlement (CE) nº 1338/2008 du Parlement européen et du Conseil ([29]).

2. En outre, aux fins du présent règlement, on entend par:

a) «données de santé électroniques à caractère personnel», les données concernant la santé et les données génétiques, qui sont traitées sous une forme électronique;

b) «données de santé électroniques à caractère non personnel», les données de santé électroniques autres que les données de santé électroniques à caractère personnel, comprenant à la fois les données qui ont été anonymisées de sorte qu'elles ne se rapportent plus à une personne physique identifiée ou identifiable («personne concernée») et les données qui ne se sont jamais rapportées à une personne concernée;

c) «données de santé électroniques», les données de santé électroniques à caractère personnel ou non personnel;

d) «utilisation primaire», le traitement de données de santé électroniques pour la fourniture de soins de santé en vue d'évaluer, de maintenir ou de rétablir l'état de santé de la personne physique à laquelle ces données se rapportent, y compris la prescription, la dispensation et la fourniture de médicaments et de dispositifs médicaux, ainsi que pour les services sociaux, administratifs ou de remboursement pertinents;

e) «utilisation secondaire», le traitement de données de santé électroniques aux fins énoncées au chapitre IV du présent règlement, autres que les finalités initiales pour lesquelles ces données ont été collectées ou produites;

f) «interopérabilité», la capacité d'organisations, ainsi que d'applications logicielles ou de dispositifs du même fabricant ou de fabricants différents, à interagir au moyen des processus qu'ils soutiennent, ce qui implique l'échange d'informations et de connaissances, sans modification du contenu des données, entre ces organisations, applications logicielles ou dispositifs;

([28]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

([29]) Règlement (CE) nº 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail (JO L 354 du 31.12.2008, p. 70).

g) «enregistrement des données de santé électroniques», l'enregistrement de données de santé dans un format électronique par la saisie manuelle de ces données, par la collecte de ces données au moyen d'un dispositif ou par la conversion dans un format électronique de données de santé non électroniques à traiter dans un système de DME ou dans une application de bien-être;

h) «service d'accès aux données de santé électroniques», un service en ligne, tel qu'un portail ou une application pour les appareils mobiles, qui permet aux personnes physiques n'agissant pas dans l'exercice de leurs fonctions professionnelles d'accéder à leurs propres données de santé électroniques ou aux données de santé électroniques d'autres personnes physiques auxquelles elles sont légalement autorisées à accéder;

i) «service d'accès des professionnels de la santé», un service qui, accompagné par un système de DME, permet aux professionnels de la santé d'accéder aux données de personnes physiques qu'ils traitent;

j) «dossier médical électronique» ou «DME», un ensemble de données de santé électroniques relatives à une personne physique collectées dans le système de santé et traitées aux fins de la prestation de soins de santé;

k) «système de dossiers médicaux électroniques» ou «système de DME», tout système dont le logiciel ou une combinaison du matériel informatique et du logiciel permet le stockage, l'intermédiation, l'exportation, l'importation, la conversion, l'édition ou la consultation de données de santé électroniques à caractère personnel qui appartiennent aux catégories prioritaires de données de santé électroniques à caractère personnel établies par le présent règlement, et qui est destiné par le fabricant à être utilisé par les prestataires de soins de santé pour dispenser des soins aux patients ou par les patients pour accéder à leurs données de santé électroniques;

l) «mise en service», la première utilisation dans l'Union, conformément à sa destination, d'un système de DME relevant du présent règlement;

m) «composant logiciel», une partie distincte d'un logiciel qui propose une fonctionnalité spécifique ou exécute des fonctions ou des procédures spécifiques et qui peut fonctionner de manière indépendante ou en lien avec d'autres composants;

n) «composant logiciel d'interopérabilité européen pour les systèmes de DME», un composant logiciel du système de DME qui fournit et reçoit des données de santé électroniques à caractère personnel relevant d'une catégorie prioritaire à des fins d'utilisation primaire établie par le présent règlement dans le format européen d'échange des dossiers médicaux électroniques prévu par le présent règlement et qui est indépendant du composant logiciel de journalisation européen pour les systèmes de DME;

o) «composant logiciel de journalisation européen pour les systèmes de DME», un composant logiciel du système de DME qui fournit des informations de journalisation liées à l'accès par des professionnels de la santé ou d'autres personnes aux catégories prioritaires des données de santé électroniques à caractère personnel établies par le présent règlement, dans le format défini au point 3.2 de son annexe II, et qui est indépendant du composant logiciel d'interopérabilité européen pour les systèmes de DME;

p) «marquage CE de conformité», un marquage par lequel le fabricant indique qu'un système de DME est conforme aux exigences applicables énoncées dans le présent règlement et dans d'autres dispositions du droit de l'Union applicables qui en prévoient l'apposition en vertu du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([30]);

q) «risque», la combinaison de la probabilité de survenance d'un danger causant un dommage à la santé, la sûreté ou la sécurité de l'information et du degré de gravité d'un tel dommage;

r) «incident grave», tout dysfonctionnement ou toute détérioration des caractéristiques ou des performances d'un système de DME mis à disposition sur le marché qui entraîne, pourrait avoir entraîné ou pourrait entraîner, directement ou indirectement:

i) le décès d'une personne physique ou un préjudice grave pour la santé d'une personne physique;

ii) des atteintes graves aux droits d'une personne physique;

iii) une perturbation grave de la gestion et de l'exploitation d'infrastructures critiques dans le secteur de la santé;

([30]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

s) «soins», un service professionnel destiné à répondre aux besoins spécifiques d'une personne physique qui, en raison d'une déficience ou de son état physique ou mental, a besoin d'une assistance, y compris des mesures de prévention et d'accompagnement, pour accomplir les activités essentielles de la vie quotidienne afin de favoriser son autonomie personnelle;

t) «détenteur de données de santé», toute personne physique ou morale, autorité publique, agence ou autre organisme dans les secteurs des soins de santé ou des soins, y compris les services de remboursement si nécessaire, ainsi que toute personne physique ou morale qui développe des produits ou des services destinés aux secteurs de la santé, des soins de santé ou des soins, qui développe ou produit des applications de bien-être, qui effectue des travaux de recherche ayant trait aux secteurs des soins de santé ou des soins, ou qui agit en tant que registre de mortalité, ainsi que toute institution ou tout organe ou organisme de l'Union, qui ont:

i) le droit ou l'obligation, conformément au droit de l'Union ou au droit national applicables et en leur qualité de responsable ou de responsable conjoint du traitement, de traiter des données de santé électroniques à caractère personnel à des fins de fourniture de soins de santé ou de soins, ou à des fins de santé publique, de remboursement, de recherche, d'innovation, d'élaboration des politiques, de statistiques officielles ou de sécurité des patients ou à des fins de réglementation; ou

ii) la capacité de mettre à disposition des données de santé électroniques à caractère non personnel par le biais du contrôle de la conception technique d'un produit et de services liés, y compris en enregistrant ou en fournissant ces données, en limitant l'accès à ces données ou en échangeant ces données;

u) «utilisateur de données de santé», une personne physique ou morale, y compris les institutions, organes ou organismes de l'Union, qui s'est vu octroyer un accès licite aux données de santé électroniques à des fins d'utilisation secondaire en vertu d'une autorisation de traitement de données, d'une approbation d'une demande de données de santé ou d'une approbation d'accès émanant d'un participant autorisé à DonnéesDeSanté@UE (HealthData@EU);

v) «autorisation de traitement de données», une décision administrative délivrée par un organisme responsable de l'accès aux données de santé à un utilisateur de données de santé, lui donnant le droit de traiter certaines données de santé électroniques indiquées dans l'autorisation de traitement de données à des fins d'utilisation secondaire spécifiques, sur la base des conditions énoncées au chapitre IV du présent règlement;

w) «ensemble de données», une collection structurée de données de santé électroniques;

x) «ensemble de données ayant une incidence majeure sur l'utilisation secondaire», un ensemble de données dont la réutilisation est associée à d'importantes retombées positives en raison de sa pertinence pour la recherche en matière de santé;

y) «catalogue des ensembles de données», une collection de descriptions d'ensembles de données, organisée de manière systématique et comprenant une partie publique orientée vers l'utilisateur, dans laquelle les informations concernant les paramètres des ensembles de données individuels sont accessibles par voie électronique par l'intermédiaire d'un portail en ligne;

z) «qualité des données», la mesure dans laquelle les éléments des données de santé électroniques conviennent à leur utilisation primaire et à leur utilisation secondaire prévues;

a *bis*) «label de qualité et d'utilité des données», un diagramme graphique comprenant une échelle et décrivant la qualité des données et les conditions d'utilisation d'un ensemble de données;

a *ter*) «application de bien-être», tout logiciel ou toute combinaison de matériel informatique et de logiciel, destiné par le fabricant à être utilisé par une personne physique, pour le traitement de données de santé électroniques, en particulier pour fournir des informations sur la santé de personnes physiques ou dispenser des soins à des fins autres que la prestation de soins de santé.

CHAPITRE II

UTILISATION PRIMAIRE

SECTION 1

Droits des personnes physiques en ce qui concerne l'utilisation primaire de leurs données de santé électroniques à caractère personnel, et dispositions y afférentes

Article 3

Droit d'accès des personnes physiques à leurs données de santé électroniques à caractère personnel

1. Les personnes physiques ont le droit d'accéder au moins aux données de santé électroniques à caractère personnel les concernant qui appartiennent aux catégories prioritaires visées à l'article 14 et qui sont traitées pour la prestation de soins de santé par l'intermédiaire des services d'accès aux données de santé électroniques visés à l'article 4. L'accès est fourni immédiatement après que les données de santé électroniques à caractère personnel ont été enregistrées dans un système de DME, tout en respectant le besoin de faisabilité technique, et les données sont fournies gratuitement et dans un format aisément lisible, consolidé et accessible.

2. Les personnes physiques, ou leurs représentants visés à l'article 4, paragraphe 2, ont le droit de télécharger gratuitement une copie électronique au moins des données de santé électroniques à caractère personnel relevant des catégories prioritaires visées à l'article 14 les concernant, par l'intermédiaire des services d'accès aux données de santé électroniques visés à l'article 4, dans le format européen d'échange des dossiers médicaux électroniques visé à l'article 15.

3. Conformément à l'article 23 du règlement (UE) 2016/679, les États membres peuvent limiter la portée des droits prévus aux paragraphes 1 et 2 du présent article, en particulier lorsque ces limitations sont nécessaires pour protéger les personnes physiques, sur la base de la sécurité des patients et de considérations éthiques, en retardant l'accès des personnes physiques à leurs données de santé électroniques à caractère personnel pendant une période limitée, jusqu'à ce qu'un professionnel de la santé puisse leur communiquer de manière adéquate des informations susceptibles d'avoir une incidence significative sur leur santé et leur donner des explications appropriées sur ces informations.

Article 4

Services d'accès aux données de santé électroniques pour les personnes physiques et leurs représentants

1. Les États membres veillent à ce qu'un ou plusieurs services d'accès aux données de santé électroniques soient mis en place au niveau national, régional ou local, permettant ainsi aux personnes physiques d'accéder à leurs données de santé électroniques à caractère personnel et d'exercer leurs droits prévus aux articles 3 et 5 à 10. Ces services d'accès aux données de santé électroniques sont gratuits pour les personnes physiques et leurs représentants visés au paragraphe 2 du présent article.

2. Les États membres veillent à ce qu'un ou plusieurs services de procuration soient mis en place en tant que fonctionnalité des services d'accès aux données de santé électroniques qui permette:

a) aux personnes physiques d'autoriser d'autres personnes physiques de leur choix à accéder à leurs données de santé électroniques à caractère personnel, ou à une partie de celles-ci, en leur nom, pour une durée limitée ou illimitée et, si nécessaire, uniquement pour une fin spécifique, et de gérer ces autorisations; et

b) aux représentants légaux de personnes physiques d'accéder aux données de santé électroniques à caractère personnel de ces personnes physiques dont ils gèrent les affaires, conformément au droit national.

Les États membres établissent des règles concernant les autorisations visées au point a) du premier alinéa et les actions des tuteurs et des autres représentants légaux.

3. Les services de procuration visés au paragraphe 2 fournissent des autorisations de manière transparente et facilement compréhensible, gratuitement, par voie électronique ou sur papier. Les personnes physiques et leurs représentants sont informés de leurs droits liés à l'autorisation, y compris de la manière d'exercer ces droits, et de la procédure d'autorisation.

Les services de procuration mettent à disposition un mécanisme de réclamation facilement accessible pour les personnes physiques.

4. Les services de procuration visés au paragraphe 2 du présent article sont interopérables d'un État membre à l'autre. La Commission établit, par voie d'actes d'exécution, les spécifications techniques pour l'interopérabilité des services de procuration des États membres. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

5. Les services d'accès aux données de santé électroniques et les services de procuration sont facilement accessibles pour les personnes handicapées, les groupes vulnérables et les personnes dotées d'une faible habileté numérique.

Article 5

Droit des personnes physiques d'insérer des informations dans leur propre DME

Les personnes physiques ou leurs représentants visés à l'article 4, paragraphe 2, ont le droit d'insérer des informations dans le DME de ces personnes physiques par l'intermédiaire des services d'accès aux données de santé électroniques ou d'applications liées à ces services visés audit article. Ces informations apparaissent clairement comme ayant été insérées par la personne physique ou par son représentant. Les personnes physiques ou leurs représentants visés à l'article 4, paragraphe 2, ne peuvent pas modifier directement les données de santé électroniques et les informations connexes qui ont été insérées par les professionnels de la santé.

Article 6

Droit des personnes physiques d'obtenir une rectification

Les services d'accès aux données de santé électroniques visés à l'article 4 permettent aux personnes physiques de demander facilement en ligne la rectification de leurs données de santé électroniques à caractère personnel conformément à l'article 16 du règlement (UE) 2016/679. Le cas échéant, le responsable du traitement des données vérifie l'exactitude des informations fournies dans la demande auprès d'un professionnel de la santé compétent.

Les États membres peuvent également permettre aux personnes physiques d'exercer en ligne d'autres droits en vertu du chapitre III du règlement (UE) 2016/679 par l'intermédiaire des services d'accès aux données de santé électroniques.

Article 7

Droit des personnes physiques à la portabilité des données

1. Les personnes physiques ont le droit de donner l'accès à tout ou partie de leurs données de santé électroniques à caractère personnel à un prestataire de soins de santé de leur choix, ou de demander à un prestataire de soins de santé de transmettre tout ou partie de celles-ci à un autre prestataire de soins de santé de leur choix, immédiatement, gratuitement et sans que le prestataire de soins de santé ou les fabricants des systèmes utilisés par celui-ci y fassent obstacle.

2. Les personnes physiques ont le droit, lorsque les prestataires de soins de santé sont situés dans différents États membres, de demander la transmission de leurs données de santé électroniques à caractère personnel dans le format européen d'échange des dossiers médicaux électroniques visé à l'article 15 par l'intermédiaire de l'infrastructure transfrontière visée à l'article 23. Le prestataire de soins de santé destinataire accepte ces données et est en mesure de les lire.

3. Les personnes physiques ont le droit de demander à un prestataire de soins de santé de transmettre une partie de leurs données de santé électroniques à caractère personnel à un destinataire clairement identifié du secteur de la sécurité sociale ou des services de remboursement. Cette transmission a lieu immédiatement, gratuitement et sans que le prestataire de soins de santé ou les fabricants des systèmes utilisés par celui-ci puissent y faire obstacle, et cette transmission ne s'effectue que dans un sens.

4. Lorsque des personnes physiques ont téléchargé une copie électronique de leurs catégories prioritaires de données de santé électroniques à caractère personnel conformément à l'article 3, paragraphe 2, elles peuvent transmettre ces données aux prestataires de soins de santé de leur choix dans le format européen d'échange des dossiers médicaux électroniques visé à l'article 15. Le prestataire de soins de santé destinataire accepte ces données et est en mesure de les lire, selon le cas.

Article 8

Droit de limiter l'accès aux données

Les personnes physiques ont le droit de limiter l'accès des professionnels de la santé et des prestataires de soins de santé à tout ou partie de leurs données de santé électroniques à caractère personnel visées à l'article 3.

Lorsqu'elles exercent le droit visé au premier alinéa, les personnes physiques sont informées qu'une telle limitation d'accès pourrait avoir une incidence sur la prestation de soins de santé à leur égard.

Le fait qu'une personne physique ait procédé à une limitation d'accès au titre du premier alinéa n'est pas visible pour les prestataires de soins de santé.

Les États membres établissent les règles et les garanties spécifiques concernant ces mécanismes de limitation.

Article 9

Droit d'obtenir des informations sur l'accès aux données

1. Les personnes physiques ont le droit d'obtenir des informations, y compris au moyen de notifications automatiques, sur tout accès à leurs données de santé électroniques à caractère personnel obtenu par l'intermédiaire du service d'accès des professionnels de la santé dans le cadre des soins de santé, y compris l'accès fourni conformément à l'article 11, paragraphe 5.

2. Les informations visées au paragraphe 1 sont fournies, gratuitement et sans retard, par l'intermédiaire des services d'accès aux données de santé électroniques et sont disponibles pendant au moins trois ans à compter de chaque date d'accès aux données. Ces informations comprennent au moins les éléments suivants:

a) des informations sur le prestataire de soins de santé ou d'autres personnes ayant eu accès aux données de santé électroniques à caractère personnel;

b) la date et l'heure de l'accès;

c) quelles données de santé électroniques à caractère personnel ont été consultées.

3. Les États membres peuvent prévoir des limitations du droit visé au paragraphe 1 dans des circonstances exceptionnelles, lorsque des éléments factuels indiquent que la divulgation de ces informations compromettrait les intérêts vitaux ou les droits du professionnel de la santé concerné ou les soins apportés à la personne physique.

Article 10

Droit de refus («opt-out») des personnes physiques dans le contexte d'une utilisation primaire

1. Les législations des États membres peuvent prévoir le droit pour les personnes physiques de refuser l'accès à leurs données de santé électroniques à caractère personnel enregistrées dans un système de DME par l'intermédiaire des services d'accès aux données de santé électroniques visés aux articles 4 et 12. Dans de tels cas, les États membres veillent à ce que l'exercice de ce droit soit réversible.

2. Lorsqu'un État membre prévoit le droit visé au paragraphe 1 du présent article, il établit les règles et les garanties spécifiques concernant ce mécanisme de refus. En particulier, les États membres peuvent prévoir qu'un prestataire de soins de santé ou un professionnel de la santé peut avoir accès aux données de santé électroniques à caractère personnel dans les cas où le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique comme visé à l'article 9, paragraphe 2, point c), du règlement (UE) 2016/679, même si le patient a exercé son droit de de refus dans le contexte d'une utilisation primaire.

Article 11

Accès des professionnels de la santé aux données de santé électroniques à caractère personnel

1. Lorsqu'ils traitent des données dans un format électronique, les professionnels de la santé ont accès aux données de santé électroniques à caractère personnel pertinentes et nécessaires des personnes physiques qu'ils traitent, par l'intermédiaire des services d'accès des professionnels de la santé visés à l'article 12, quels que soient l'État membre d'affiliation et l'État membre de traitement.

2. Lorsque l'État membre d'affiliation de la personne physique traitée et l'État membre de traitement de cette personne physique diffèrent, l'accès transfrontière aux données de santé électroniques à caractère personnel de la personne physique traitée est fourni par l'intermédiaire de l'infrastructure transfrontière visée à l'article 23.

3. L'accès visé aux paragraphes 1 et 2 du présent article comprend au minimum les catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14.

Conformément aux principes prévus à l'article 5 du règlement (UE) 2016/679, les États membres établissent des règles prévoyant les catégories de données de santé électroniques à caractère personnel qui sont accessibles par les différentes catégories de professionnels de la santé ou pour les différentes tâches liées aux soins de santé. Ces règles tiennent compte de la possibilité d'imposer des limitations au titre de l'article 8 du présent règlement.

4. En cas de traitement dans un État membre autre que l'État membre d'affiliation, les règles visées au paragraphe 3 sont celles de l'État membre de traitement.

5. Lorsque l'accès aux données de santé électroniques à caractère personnel a été limité par une personne physique en vertu de l'article 8, le prestataire de soins de santé ou le professionnel de la santé n'est pas informé du contenu limité de ces données.

Par dérogation au premier alinéa de l'article 8, le prestataire de soins de santé ou le professionnel de la santé peut se voir octroyer l'accès aux données de santé électroniques auxquelles l'accès a été limité si cela s'avère nécessaire pour protéger les intérêts vitaux de la personne concernée. Ces événements sont enregistrés dans un format clair et compréhensible et sont facilement accessibles à la personne concernée.

Les États membres peuvent prévoir des garanties supplémentaires.

Article 12

Services d'accès des professionnels de la santé

Pour la prestation de soins de santé, les États membres veillent à ce que les professionnels de la santé puissent accéder gratuitement aux catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14, y compris pour les soins transfrontières, par l'intermédiaire des services d'accès des professionnels de la santé.

Les services visés au premier alinéa du présent article ne sont accessibles qu'aux professionnels de la santé qui sont en possession de moyens d'identification électronique qui font l'objet d'une reconnaissance en vertu de l'article 6 du règlement (UE) nº 910/2014 ou d'autres moyens d'identification électronique conformes aux spécifications communes visées à l'article 36 du présent règlement.

Les données de santé électroniques à caractère personnel sont présentées de manière conviviale dans les dossiers médicaux électroniques, afin de permettre une utilisation aisée par les professionnels de la santé.

Article 13

Enregistrement des données de santé électroniques à caractère personnel

1. Lorsque des données de santé électroniques sont traitées pour la prestation de soins de santé, les États membres veillent à ce que les prestataires de soins de santé enregistrent, dans un format électronique dans un système de DME, les données de santé électroniques à caractère personnel pertinentes relevant en tout ou en partie au moins des catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14.

2. Les prestataires de soins de santé qui traitent des données dans un format électronique veillent à ce que les données de santé électroniques à caractère personnel des personnes physiques qu'ils traitent soient mises à jour à l'aide d'informations liées aux soins de santé.

3. Lorsque des données de santé électroniques à caractère personnel sont enregistrées dans un État membre de traitement qui diffère de l'État membre d'affiliation de la personne physique concernée, l'État membre de traitement veille à ce que l'enregistrement soit effectué avec les données d'identification de la personne physique dans l'État membre d'affiliation.

4. Au plus tard le 26 mars 2027, la Commission détermine, par voie d'actes d'exécution, les exigences en matière de qualité des données, y compris en ce qui concerne la sémantique, l'uniformité, la cohérence, l'exactitude et l'exhaustivité, pour l'enregistrement des données de santé électroniques à caractère personnel dans un système de DME, comme il convient. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Lorsque des données de santé électroniques à caractère personnel sont enregistrées ou mises à jour, les dossiers médicaux électroniques indiquent le professionnel de la santé et le prestataire de soins de santé qui a procédé à cet enregistrement ou à cette mise à jour, ainsi que l'heure à laquelle cet enregistrement ou cette mise à jour a eu lieu. Les États membres peuvent exiger qu'il soit gardé trace d'autres aspects de l'enregistrement des données.

Article 14

Catégories prioritaires de données de santé électroniques à caractère personnel à des fins d'utilisation primaire

1. Aux fins du présent chapitre, lorsque les données sont traitées dans un format électronique, les catégories prioritaires de données de santé électroniques à caractère personnel sont les suivantes:

a) résumés des dossiers de patients;

b) prescriptions électroniques;

c) dispensations électroniques;

d) examens d'imagerie médicale et comptes rendus d'imagerie médicale y afférents;

e) résultats d'examens médicaux, y compris les résultats de laboratoire et d'autres diagnostics, ainsi que les comptes rendus y afférents; et

f) rapports de sortie d'hôpital.

Les principales caractéristiques des catégories prioritaires de données de santé électroniques à caractère personnel à des fins d'utilisation primaire figurent à l'annexe I.

Les États membres peuvent prévoir, dans leur droit national, l'accès à des catégories de données de santé électroniques à caractère personnel supplémentaires et leur échange, à des fins d'utilisation primaire en application du présent chapitre.

La Commission peut, par voie d'actes d'exécution, établir des spécifications transfrontières pour les catégories de données de santé électroniques à caractère personnel visées au troisième alinéa du présent paragraphe en vertu de l'article 15, paragraphe 3, et de l'article 23, paragraphe 8. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier le présent règlement en modifiant l'annexe I par l'ajout, la modification ou la suppression des principales caractéristiques des catégories prioritaires de données de santé électroniques à caractère personnel visées au paragraphe 1, pour autant que les modifications visent à adapter les catégories prioritaires de données de santé électroniques à caractère personnel à l'évolution technique et aux normes internationales. Par ailleurs, les ajouts et les modifications de ces caractéristiques satisfont aux deux critères suivants:

a) la caractéristique est pertinente pour les soins de santé dispensés à des personnes physiques;

b) la caractéristique est utilisée dans la majorité des États membres selon les informations les plus récentes.

Article 15

Format européen d'échange des dossiers médicaux électroniques

1. Au plus tard le 26 mars 2027, la Commission établit, par voie d'actes d'exécution, les spécifications techniques pour les catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14, paragraphe 1, en fixant le format européen d'échange des dossiers médicaux électroniques. Ce format est un format couramment utilisé et lisible par machine, qui permet la transmission de données de santé électroniques à caractère personnel entre différents dispositifs, applications logicielles et prestataires de soins de santé. Un tel format soutient la transmission de données de santé structurées et non structurées, et comprend les éléments suivants:

a) des ensembles de données harmonisés contenant des données de santé électroniques et définissant des structures, telles que des champs de données et des groupes de données pour la représentation de contenu clinique et d'autres parties des données de santé électroniques;

b) des systèmes de codage et des valeurs à utiliser dans les ensembles de données contenant des données de santé électroniques;

c) des spécifications techniques d'interopérabilité pour l'échange de données de santé électroniques, y compris la représentation de son contenu, les normes et les profils.

Les actes d'exécution visés au premier alinéa du présent paragraphe sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. La Commission met régulièrement à jour le format européen d'échange des dossiers médicaux électroniques par voie d'actes d'exécution afin d'intégrer les révisions pertinentes des nomenclatures et systèmes de codage des soins de santé. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

3. La Commission peut, par voie d'actes d'exécution, établir des spécifications techniques pour étendre le format européen d'échange des dossiers médicaux électroniques à des catégories de données de santé électroniques à caractère personnel supplémentaires visées à l'article 14, paragraphe 1, troisième alinéa. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

4. Les États membres veillent à ce que les catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14 soient émises dans le format européen d'échange des dossiers médicaux électroniques visé au paragraphe 1 du présent article. Lorsque ces données sont transmises par des procédés automatisés à des fins d'utilisation primaire, le prestataire destinataire accepte le format des données et est en mesure de lire les données.

Article 16

Gestion de l'identification

1. Lorsque des personnes physiques utilisent des services d'accès aux données de santé électroniques visés à l'article 4, ces personnes physiques ont le droit de s'identifier par voie électronique en utilisant tout moyen d'identification électronique reconnu en vertu de l'article 6 du règlement (UE) nº 910/2014. Les États membres peuvent prévoir des mécanismes complémentaires pour garantir une mise en correspondance appropriée des identités dans les situations transfrontières.

2. La Commission détermine, par voie d'actes d'exécution, les exigences applicables au mécanisme interopérable et transfrontière d'identification et d'authentification pour les personnes physiques et les professionnels de la santé, conformément au règlement (UE) nº 910/2014. Ce mécanisme facilite la transférabilité des données de santé électroniques à caractère personnel dans un contexte transfrontière. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

3. La Commission, en coopération avec les États membres, met en œuvre, à l'échelon de l'Union, les services requis par le mécanisme interopérable et transfrontière d'identification et d'authentification visé au paragraphe 2 du présent article, dans le cadre de l'infrastructure transfrontière visée à l'article 23.

4. Les autorités compétentes des États membres et la Commission mettent en œuvre le mécanisme interopérable transfrontière d'identification et d'authentification, à l'échelon des États membres et à l'échelon de l'Union, respectivement.

Article 17

Exigences concernant la mise en œuvre technique

La Commission détermine, par voie d'actes d'exécution, les exigences concernant la mise en œuvre technique des droits énoncés dans la présente section.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 18

Indemnisation pour la mise à disposition de données de santé électroniques à caractère personnel

Les prestataires qui reçoivent des données dans le cadre du présent chapitre ne sont pas tenus d'indemniser le prestataire de soins de santé pour la mise à disposition de données de santé électroniques à caractère personnel. Un prestataire de soins de santé ou un tiers ne saurait facturer directement ou indirectement aux personnes concernées des frais ou des coûts ni exiger une indemnisation pour le partage de données ou pour l'accès à des données.

SECTION 2

Gouvernance pour l'utilisation primaire

Article 19

Autorités de santé numérique

1. Chaque État membre désigne une ou plusieurs autorités de santé numérique responsables de la mise en œuvre et de l'exécution du présent chapitre à l'échelon national. Les États membres communiquent à la Commission l'identité des autorités de santé numérique au plus tard le 26 mars 2027. Lorsqu'un État membre désigne plus d'une autorité de santé numérique ou lorsque l'autorité de santé numérique est composée de plusieurs organisations, l'État membre concerné communique à la Commission une description de la répartition des tâches entre ces différentes autorités ou organisations. Lorsqu'un État membre désigne plusieurs autorités de santé numérique, il désigne l'une d'entre elles pour agir en qualité de coordonnateur. La Commission met ces informations à la disposition du public.

2. Chaque autorité de santé numérique se voit confier les tâches et les pouvoirs suivants:

a) assurer la mise en œuvre des droits et obligations prévus au présent chapitre et au chapitre III en adoptant les solutions techniques nationales, régionales ou locales nécessaires et en établissant des règles et des mécanismes pertinents;

b) veiller à ce que des informations complètes et actualisées sur la mise en œuvre des droits et obligations prévus au présent chapitre et au chapitre III soient mises à la disposition des personnes physiques, des professionnels de la santé et des prestataires de soins de santé;

c) lors de la mise en œuvre des solutions techniques visées au point a) du présent paragraphe, veiller à ce que ces solutions techniques soient conformes au présent chapitre, au chapitre III et à l'annexe II;

d) contribuer, à l'échelon de l'Union, au développement de solutions techniques permettant aux personnes physiques et aux professionnels de la santé d'exercer leurs droits et de se conformer à leurs obligations, énoncés dans le présent chapitre;

e) faciliter l'exercice par les personnes handicapées de leurs droits prévus au présent chapitre conformément à la directive (UE) 2019/882 du Parlement européen et du Conseil ([31]);

f) superviser les points de contact nationaux pour la santé numérique et coopérer avec d'autres autorités de santé numérique et avec la Commission en vue de poursuivre le développement de MaSanté@UE (MyHealth@EU);

g) assurer, à l'échelon national, la mise en œuvre du format européen d'échange des dossiers médicaux électroniques, en coopération avec les autorités nationales et les parties prenantes;

h) contribuer, à l'échelon de l'Union, au développement du format européen d'échange des dossiers médicaux électroniques, à l'élaboration de spécifications communes, conformément à l'article 36, qui répondent aux préoccupations en matière de qualité, d'interopérabilité, de sécurité, de sûreté, de facilité d'utilisation, d'accessibilité, de non-discrimination ou de droits fondamentaux, et à l'élaboration des spécifications relatives à la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être visée à l'article 49;

i) le cas échéant, effectuer des activités de surveillance du marché conformément à l'article 43, tout en veillant à éviter tout conflit d'intérêts;

j) renforcer les capacités nationales de mise en œuvre des exigences en matière d'interopérabilité et de sécurité des données de santé électroniques à des fins d'utilisation primaire et participer aux échanges d'informations et aux activités de renforcement des capacités à l'échelle de l'Union;

k) coopérer avec les autorités de surveillance du marché, participer aux activités liées à la gestion des risques présentés par les systèmes de DME et des incidents graves, et superviser la mise en œuvre de mesures correctives conformément à l'article 44;

l) coopérer avec d'autres entités et organismes compétents à l'échelon local, régional, national ou de l'Union afin de garantir l'interopérabilité, la portabilité et la sécurité des données de santé électroniques;

([31]) Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

m) coopérer avec les autorités de contrôle conformément aux règlements (UE) nº 910/2014 et (UE) 2016/679 et à la directive (UE) 2022/2555 du Parlement européen et du Conseil ([32]) et avec d'autres autorités concernées, y compris celles compétentes en matière de cybersécurité et d'identification électronique.

3. Chaque État membre veille à ce que chaque autorité de santé numérique dispose des ressources humaines, techniques et financières, des locaux et des infrastructures nécessaires à la bonne exécution de ses tâches et à l'exercice efficace de ses pouvoirs.

4. Dans l'exécution de ses tâches, chaque autorité de santé numérique évite tout conflit d'intérêts. Chaque membre du personnel de l'autorité de santé numérique agit dans l'intérêt public et de manière indépendante.

5. Dans l'exécution de leurs tâches, les autorités de santé numérique concernées coopèrent activement et se concertent avec les représentants des parties prenantes concernées, y compris les représentants de patients, les représentants des prestataires de soins de santé et des professionnels de la santé, notamment les associations de professionnels de la santé, ainsi que les organisations de consommateurs et les associations professionnelles.

Article 20

Rapports des autorités de santé numérique

Les autorités de santé numérique désignées en vertu de l'article 19 publient tous les deux ans un rapport d'activité contenant une vue d'ensemble complète de leurs activités. Si un État membre désigne plus d'une autorité de santé numérique, l'une d'entre elles est responsable de l'élaboration du rapport et, à cette fin, demande les informations nécessaires aux autres autorités de santé numérique. Ce rapport d'activité suit une structure convenue à l'échelon de l'Union, au sein du comité de l'espace européen des données de santé (ci-après dénommé «comité de l'EEDS») visé à l'article 92. Ce rapport d'activité contient au moins des informations concernant:

a) les mesures prises pour mettre en œuvre le présent règlement;

b) le pourcentage de personnes physiques ayant accès aux différentes catégories de données de leurs dossiers médicaux électroniques;

c) le traitement des demandes des personnes physiques relatives à l'exercice de leurs droits en vertu du présent règlement;

d) le nombre de prestataires de soins de santé de différents types, y compris les pharmacies, les hôpitaux et les autres lieux où des soins sont dispensés, connectés à MaSanté@UE (MyHealth@EU), calculé:

   i) en valeur absolue;

   ii) en un pourcentage de l'ensemble des prestataires de soins de santé du même type; et

   iii) en un pourcentage des personnes physiques pouvant utiliser les services;

e) les volumes de données de santé électroniques de différentes catégories partagées par-delà les frontières au moyen de MaSanté@UE (MyHealth@EU);

f) le nombre de cas de non-conformité avec des exigences obligatoires.

Article 21

Droit d'introduire une réclamation auprès d'une autorité de santé numérique

1. Sans préjudice de tout autre recours administratif ou judiciaire, les personnes physiques et morales ont le droit d'introduire une réclamation en lien avec les dispositions du présent chapitre, individuellement ou, le cas échéant, collectivement, auprès de l'autorité de santé numérique compétente, pour autant que leurs droits ou intérêts soient lésés.

2. Lorsque la réclamation concerne les droits de personnes physiques découlant des articles 3 et 5 à 10 du présent règlement, l'autorité de santé numérique transmet la réclamation aux autorités de contrôle compétentes au titre du règlement (UE) 2016/679. L'autorité de santé numérique fournit à l'autorité de contrôle compétente au titre du règlement (UE) 2016/679 les informations nécessaires dont elle dispose afin de faciliter l'évaluation et l'enquête portant sur la réclamation.

([32]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

3. L'autorité de santé numérique compétente auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation, conformément au droit national, des progrès réalisés dans le traitement de la réclamation, de la décision prise au sujet de la réclamation, du renvoi éventuel de la réclamation à l'autorité de contrôle compétente au titre du règlement (UE) 2016/679 et, dans le cas d'un tel renvoi, de ce que l'autorité de contrôle est, à partir de ce moment, le seul point de contact pour l'auteur de la réclamation en la matière.

4. Les autorités de santé numérique des États membres concernés coopèrent pour traiter les réclamations liées à l'échange transfrontière de données de santé électroniques à caractère personnel et à l'accès à ces données et pour y apporter une réponse, y compris en échangeant toutes les informations pertinentes par voie électronique, dans les meilleurs délais.

5. Les autorités de santé numérique facilitent l'introduction de réclamations et fournissent des outils facilement accessibles pour l'introduction de réclamations.

Article 22

Relations avec les autorités de contrôle au titre du règlement (UE) 2016/679

L'autorité de contrôle ou les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 et de veiller au respect de celui-ci sont également compétentes pour surveiller l'application des articles 3 et 5 à 10 du présent règlement et pour veiller au respect desdits articles. Les dispositions pertinentes du règlement (UE) 2016/679 s'appliquent mutatis mutandis. Les autorités de contrôle disposent du pouvoir d'imposer des amendes administratives à concurrence du montant visé à l'article 83, paragraphe 5, du règlement (UE) 2016/679.

Le cas échéant, les autorités de contrôle visées au premier alinéa du présent article et les autorités de santé numérique visées à l'article 19 coopèrent aux fins de l'exécution du présent règlement, dans le cadre de leurs compétences respectives.

SECTION 3

Infrastructure transfrontière pour l'utilisation primaire des données de santé électroniques à caractère personnel

Article 23

MaSanté@UE (MyHealth@EU)

1. La Commission met en place une plateforme centrale d'interopérabilité pour la santé numérique (MaSanté@UE (MyHealth@EU)] afin de fournir des services visant à soutenir et à faciliter l'échange de données de santé électroniques à caractère personnel entre les points de contact nationaux pour la santé numérique des États membres.

2. Chaque État membre désigne un point de contact national pour la santé numérique, en tant que portail organisationnel et technique pour la fourniture de services liés à l'échange transfrontière de données de santé électroniques à caractère personnel dans le contexte d'une utilisation primaire. Chaque point de contact national pour la santé numérique est connecté à tous les autres points de contact nationaux pour la santé numérique des autres États membres et à la plateforme centrale d'interopérabilité pour la santé numérique dans l'infrastructure transfrontière MaSanté@UE (MyHealth@EU). Lorsqu'un point de contact national pour la santé numérique est une entité composée de plusieurs organisations chargées de la mise en œuvre de différents services, l'État membre concerné communique à la Commission une description de la répartition des tâches entre les organisations. Chaque État membre informe la Commission de l'identité de son point de contact national pour la santé numérique au plus tard le 26 mars 2027. Le point de contact national pour la santé numérique peut être désigné au sein de l'autorité de santé numérique visée à l'article 19. Les États membres informent la Commission de toute modification ultérieure de l'identité de ces points de contact nationaux pour la santé numérique. La Commission et les États membres mettent ces informations à la disposition du public.

3. Chaque point de contact national pour la santé numérique permet l'échange des données de santé électroniques à caractère personnel visées à l'article 14, paragraphe 1, avec des points de contact nationaux pour la santé numérique d'autres États membres par l'intermédiaire de MaSanté@UE (MyHealth@EU). Cet échange se fonde sur le format européen d'échange des dossiers médicaux électroniques.

Lorsque les États membres prévoient des catégories de données de santé électroniques à caractère personnel supplémentaires au titre de l'article 14, paragraphe 1, troisième alinéa, le point de contact national pour la santé numérique permet l'échange des catégories de données de santé électroniques à caractère personnel supplémentaires visées à l'article 14, paragraphe 1, troisième alinéa, dans la mesure où l'État membre concerné a prévu l'accès à ces catégories de données de santé électroniques à caractère personnel supplémentaires et leur échange conformément à l'article 14, paragraphe 1, troisième alinéa.

4. Au plus tard le 26 mars 2027, la Commission adopte, par voie d'actes d'exécution, les mesures nécessaires au développement technique de MaSanté@UE (MyHealth@EU), des règles détaillées concernant la sécurité, la confidentialité et la protection des données de santé électroniques à caractère personnel et les conditions applicables aux contrôles de conformité nécessaires pour adhérer et rester connecté à MaSanté@UE (MyHealth@EU). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

5. Les États membres veillent à ce que tous les prestataires de soins de santé soient connectés à leur point de contact national pour la santé numérique. Les États membres veillent à ce que les prestataires de soins de santé connectés soient en mesure de procéder à des échanges bidirectionnels de données de santé électroniques avec le point de contact national pour la santé numérique.

6. Les États membres veillent à ce que les pharmacies exerçant des activités sur leur territoire, y compris les pharmacies en ligne, soient en mesure de délivrer des prescriptions électroniques établies dans d'autres États membres, dans les conditions prévues à l'article 11 de la directive 2011/24/UE.

Les pharmacies ont accès aux prescriptions électroniques que leur transmettent d'autres États membres par l'intermédiaire de MaSanté@UE (MyHealth@EU) et les acceptent, pour autant que les conditions prévues à l'article 11 de la directive 2011/24/UE soient remplies.

À la suite de la délivrance de médicaments sur la base d'une prescription électronique provenant d'un autre État membre, la pharmacie concernée notifie, par l'intermédiaire de MaSanté@UE (MyHealth@EU), cette délivrance au point de contact pour la santé numérique de l'État membre dans lequel la prescription a été établie.

7. Les points de contact nationaux pour la santé numérique agissent en tant que responsables conjoints du traitement des données de santé électroniques à caractère personnel communiquées par l'intermédiaire de MaSanté@UE (MyHealth@EU) pour les opérations de traitement auxquelles ils participent. La Commission agit en qualité de sous-traitant.

8. La Commission, par voie d'actes d'exécution, établit les règles relatives aux exigences en matière de cybersécurité, d'interopérabilité technique, d'interopérabilité sémantique, d'opérations et de gestion des services en ce qui concerne le traitement par le sous-traitant visé au paragraphe 7 du présent article et ses responsabilités à l'égard des responsables du traitement, conformément au chapitre IV du règlement (UE) 2016/679. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

9. Les points de contact nationaux pour la santé numérique remplissent les conditions pour adhérer et rester connecté à MaSanté@UE (MyHealth@EU) prévues dans les actes d'exécution visés au paragraphe 4. La Commission vérifie le respect de ces conditions par les points de contact nationaux pour la santé numérique au moyen de contrôles de conformité.

Article 24

Services et infrastructures de santé numérique transfrontières supplémentaires

1. Les États membres peuvent fournir, par l'intermédiaire de MaSanté@UE (MyHealth@EU), des services supplémentaires facilitant la télémédecine, la santé mobile, l'accès des personnes physiques à des traductions existantes de leurs données de santé, l'échange ou la vérification de certificats liés à la santé, y compris des services de carnets de vaccination soutenant la santé publique, la surveillance de la santé publique ou les systèmes de santé numérique, ou des services et applications interopérables, en vue d'atteindre un niveau élevé de confiance et de sécurité, de renforcer la continuité des soins et de garantir l'accès à des soins de santé sûrs et de qualité. La Commission définit, par voie d'actes d'exécution, les aspects techniques de ces services supplémentaires. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. La Commission et les États membres peuvent faciliter l'échange de données de santé électroniques à caractère personnel avec d'autres infrastructures, telles que le système de gestion des données cliniques des patients ou d'autres services ou infrastructures dans les domaines de la santé, des soins ou de la sécurité sociale qui peuvent devenir des participants autorisés à MaSanté@UE (MyHealth@EU). La Commission définit, par voie d'actes d'exécution, les aspects techniques de ces échanges. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

La connexion d'une autre infrastructure à la plateforme centrale pour la santé numérique, ainsi que sa déconnexion de ladite plateforme, font l'objet d'une décision de la Commission adoptée par la voie d'un acte d'exécution, fondée sur les résultats des contrôles de conformité des aspects techniques des échanges visés au premier alinéa du présent paragraphe. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

3. Un point de contact national pour la santé numérique d'un pays tiers ou un système établi à l'échelon international par une organisation internationale peut devenir un participant autorisé à MaSanté@UE (MyHealth@EU), à condition qu'il satisfasse aux exigences de MaSanté@UE (MyHealth@EU) aux fins de l'échange de données de santé électroniques à caractère personnel visé à l'article 23, que le transfert résultant de la connexion à MaSanté@UE (MyHealth@EU) respecte les règles du chapitre V du règlement (UE) 2016/679, et que les exigences concernant les mesures juridiques, organisationnelles, opérationnelles, sémantiques, techniques et de cybersécurité soient équivalentes à celles applicables aux États membres dans le cadre du fonctionnement des services MaSanté@UE (MyHealth@EU). Ces exigences sont vérifiées par la Commission au moyen de contrôles de conformité.

Sur la base des résultats des contrôles de conformité visés au premier alinéa du présent paragraphe, la Commission peut, par voie d'actes d'exécution, décider de connecter le point de contact national pour la santé numérique du pays tiers ou le système établi à l'échelon international par une organisation internationale, selon le cas, à MaSanté@UE (MyHealth@EU), ou de l'en déconnecter. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

La Commission établit et tient à jour une liste des points de contact nationaux pour la santé numérique des pays tiers ou des systèmes établis à l'échelon international par des organisations internationales qui sont connectés à MaSanté@UE (MyHealth@EU) en vertu du présent paragraphe et met cette liste à la disposition du public.

CHAPITRE III

SYSTÈMES DE DME ET APPLICATIONS DE BIEN-ÊTRE

SECTION 1

Champ d'application et dispositions générales relatives aux systèmes de DME

Article 25

Composants logiciels harmonisés des systèmes de DME

1. Les systèmes de DME comprennent un composant logiciel d'interopérabilité européen pour les systèmes de DME et un composant logiciel de journalisation européen pour les systèmes de DME (ci-après dénommés «composants logiciels harmonisés des systèmes de DME»), conformément aux dispositions du présent chapitre.

2. Le présent chapitre ne s'applique pas aux logiciels à usage général utilisés dans un environnement de soins de santé.

Article 26

Mise sur le marché et mise en service

1. Les systèmes de DME ne sont mis sur le marché ou mis en service que s'ils respectent les dispositions du présent chapitre.

2. Les systèmes de DME fabriqués et utilisés dans les établissements de santé établis dans l'Union, ainsi que les systèmes de DME proposés en tant que service, tel que ce terme est défini à l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([33]), à une personne physique ou morale établie dans l'Union, sont considérés comme ayant été mis en service.

3. Les États membres ne peuvent pas interdire ni restreindre la mise sur le marché des systèmes de DME qui respectent le présent règlement, pour des considérations relatives aux aspects concernant les composants logiciels harmonisés des systèmes de DME réglementés par le présent règlement.

Article 27

Relations avec le droit de l'Union régissant les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro et les systèmes d'IA

1. Les fabricants de dispositifs médicaux ou de dispositifs médicaux de diagnostic in vitro, tels qu'ils sont définis, respectivement, à l'article 2, point 1), du règlement (UE) 2017/745 et à l'article 2, point 2), du règlement (UE) 2017/746, qui allèguent l'interopérabilité de ces dispositifs médicaux ou de ces dispositifs médicaux de diagnostic in vitro avec les composants logiciels harmonisés des systèmes de DME prouvent que lesdits dispositifs sont conformes aux exigences

([33]) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

essentielles applicables au composant logiciel d'interopérabilité européen pour les systèmes de DME et au composant logiciel de journalisation européen pour les systèmes de DME fixées à la section 2 de l'annexe II du présent règlement. L'article 36 du présent règlement s'applique à ces dispositifs médicaux et à ces dispositifs médicaux de diagnostic in vitro.

2. Les fournisseurs de systèmes d'IA qui sont considérés comme étant à haut risque conformément à l'article 6 du règlement (UE) 2024/1689 (ci-après dénommés «systèmes d'IA à haut risque») et qui ne relèvent pas du champ d'application du règlement (UE) 2017/745 ou (UE) 2017/746, qui allèguent l'interopérabilité de ces systèmes d'IA à haut risque avec les composants logiciels harmonisés des systèmes de DME prouvent que lesdits systèmes sont conformes aux exigences essentielles applicables au composant logiciel d'interopérabilité européen pour les systèmes de DME et au composant logiciel de journalisation européen pour les systèmes de DME fixées à la section 2 de l'annexe II du présent règlement. L'article 36 du présent règlement s'applique à ces systèmes d'IA à haut risque.

Article 28

Allégations

Dans la fiche d'information, la notice d'utilisation ou toute autre information accompagnant les systèmes de DME, ainsi que dans la publicité pour les systèmes de DME, il est interdit d'utiliser du texte, des noms, des marques commerciales, des images ou des signes figuratifs ou d'autres signes susceptibles d'induire en erreur l'utilisateur professionnel, tel qu'il est défini à l'article 3, point 8), du règlement (UE) 2018/1807 du Parlement européen et du Conseil ([34]), en ce qui concerne la destination, l'interopérabilité et la sécurité desdits systèmes:

a) en attribuant au système de DME des fonctions et des propriétés dont ledit système est dépourvu;

b) en n'informant pas l'utilisateur professionnel des limitations probables liées à l'interopérabilité ou aux dispositifs de sécurité du système de DME par rapport à sa destination;

c) en suggérant des utilisations du système de DME autres que celles déclarées comme relevant de la destination dans la documentation technique.

Article 29

Acquisition, remboursement et financement

Les États membres peuvent maintenir ou définir des règles spécifiques pour l'acquisition, le financement ou le remboursement de systèmes de DME dans le contexte de l'organisation, de la fourniture ou du financement de services de soins de santé, à condition que ces règles soient conformes au droit de l'Union et n'affectent pas le fonctionnement ou la conformité des composants logiciels harmonisés des systèmes de DME.

SECTION 2

Obligations des opérateurs économiques en ce qui concerne les systèmes de DME

Article 30

Obligations des fabricants de systèmes de DME

1. Les fabricants de systèmes de DME:

a) veillent à ce que les composants logiciels harmonisés de leurs systèmes de DME et les systèmes de DME eux-mêmes, dans la mesure où le présent chapitre établit des exigences les concernant, soient conformes aux exigences essentielles fixées à l'annexe II et aux spécifications communes visées à l'article 36;

b) veillent à ce que les composants logiciels harmonisés de leurs systèmes de DME ne subissent pas d'effets négatifs d'autres composants logiciels du même système de DME;

c) établissent la documentation technique de leurs systèmes de DME conformément à l'article 37 avant de mettre ces systèmes de DME sur le marché, et tiennent cette documentation à jour par la suite;

([34]) Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (JO L 303 du 28.11.2018, p. 59).

d) veillent à ce que leurs systèmes de DME soient accompagnés, gratuitement pour l'utilisateur, de la fiche d'information prévue à l'article 38 et d'une notice d'utilisation claire et complète;

e) établissent la déclaration UE de conformité conformément à l'article 39;

f) apposent le marquage CE de conformité conformément à l'article 41;

g) indiquent le nom, la raison sociale ou la marque déposée, l'adresse postale et le site internet, l'adresse électronique ou d'autres coordonnées numériques grâce auxquels ils peuvent être contactés, dans le système de DME; indiquent dans les coordonnées un point unique auquel le fabricant peut être contacté; les coordonnées sont rédigées dans une langue qui peut être aisément comprise par les utilisateurs et les autorités de surveillance du marché;

h) respectent les obligations d'enregistrement prévues à l'article 49;

i) prennent sans retard indu toute mesure corrective nécessaire en ce qui concerne leurs systèmes de DME, lorsqu'ils estiment ou ont des raisons de croire que lesdits systèmes ne sont pas ou ne sont plus conformes aux exigences essentielles fixées à l'annexe II, ou rappellent ou retirent ces systèmes; les fabricants de systèmes de DME informent ensuite les autorités nationales des États membres dans lesquels ils ont mis leurs systèmes de DME à disposition sur le marché ou dans lesquels ils les ont mis en service, de la non-conformité, de toute mesure corrective prise, y compris le calendrier de mise en œuvre, et de la date à laquelle les composants logiciels harmonisés de leurs systèmes de DME ont été mis en conformité ou rappelés ou retirés;

j) informent les distributeurs de leurs systèmes de DME et, le cas échéant, le mandataire, les importateurs et les utilisateurs de la non-conformité et de toute mesure corrective ou de tout rappel ou retrait de ces systèmes de DME;

k) informent les distributeurs de leurs systèmes de DME et, le cas échéant, le mandataire, les importateurs et les utilisateurs de toute maintenance préventive obligatoire des systèmes de DME et de sa fréquence;

l) fournissent, à la demande et dans une langue officielle de l'État membre concerné, aux autorités de surveillance du marché de cet État membre, toutes les informations et tous les documents qui sont nécessaires pour démontrer la conformité des systèmes de DME qu'ils ont mis sur le marché ou mis en service aux exigences essentielles fixées à l'annexe II;

m) coopèrent avec les autorités de surveillance du marché, à leur demande, en vue de prendre toute mesure permettant de mettre les systèmes de DME qu'ils ont mis sur le marché ou mis en service en conformité avec les exigences essentielles fixées à l'annexe II et avec les exigences éventuelles adoptées en vertu de l'article 42 dans une langue officielle de l'État membre concerné;

n) mettent en place des canaux de réclamation et en tiennent les distributeurs informés;

o) tiennent un registre des réclamations et un registre des systèmes de DME non conformes, et en tiennent les distributeurs informés.

2. Les fabricants de systèmes de DME veillent à ce que des procédures soient en place pour garantir que la conception, le développement et le déploiement des composants logiciels harmonisés d'un système de DME continuent d'être conformes aux exigences essentielles fixées à l'annexe II et aux spécifications communes visées à l'article 36. Les modifications de la conception ou des caractéristiques d'un système de DME en ce qui concerne les composants logiciels harmonisés d'un système de DME sont dûment prises en compte et reflétées dans la documentation technique.

3. Les fabricants de systèmes de DME conservent la documentation technique visée à l'article 37 et la déclaration UE de conformité visée à l'article 39 pendant une période de dix ans après la mise sur le marché du système de DME couvert par la déclaration UE de conformité.

Les fabricants de systèmes de DME mettent à la disposition des autorités concernées, le code source ou la logique de programmation figurant dans la documentation technique, sur requête motivée, si ce code source ou cette logique de programmation est nécessaire pour permettre à ces autorités de vérifier la conformité aux exigences essentielles fixées à l'annexe II.

4. Les fabricants de systèmes de DME établis en dehors de l'Union veillent à ce que leur mandataire dispose facilement des documents nécessaires afin d'exécuter les tâches visées à l'article 31, paragraphe 2.

5. Sur requête motivée d'une autorité de surveillance du marché, les fabricants de systèmes de DME communiquent à cette autorité de surveillance du marché, sur support papier ou sous format électronique, toutes les informations et tous les documents nécessaires pour démontrer la conformité du système de DME aux exigences essentielles fixées à l'annexe II ainsi qu'aux spécifications communes visées à l'article 36, dans une langue qui peut être aisément comprise par cette autorité de surveillance du marché. Les fabricants de systèmes de DME coopèrent avec l'autorité de surveillance du marché, à sa demande, concernant toute mesure prise pour éliminer les risques présentés par un système de DME qu'ils ont mis sur le marché ou mis en service.

Article 31

Mandataires

1. Avant de mettre un système de DME à disposition sur le marché de l'Union, un fabricant d'un système de DME établi en dehors de l'Union désigne, par mandat écrit, un mandataire qui est établi dans l'Union.

2. Le mandataire exécute les tâches spécifiées dans le mandat convenu avec le fabricant. Le mandat autorise le mandataire à faire au minimum ce qui suit:

a) tenir la déclaration UE de conformité et la documentation technique visée à l'article 37 à la disposition des autorités de surveillance du marché pendant la durée prévue à l'article 30, paragraphe 3;

b) à la suite d'une demande motivée d'une autorité de surveillance du marché, communiquer aux autorités de l'État membre concerné une copie du mandat et toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système de DME aux exigences essentielles fixées à l'annexe II ainsi qu'aux spécifications communes visées à l'article 36;

c) informer sans retard indu le fabricant si le mandataire a des raisons de croire qu'un système de DME n'est plus conforme aux exigences essentielles fixées à l'annexe II;

d) informer sans retard indu le fabricant de toute réclamation reçue de consommateurs ou d'utilisateurs professionnels;

e) coopérer avec les autorités de surveillance du marché, à leur demande, en vue de prendre toute mesure corrective en rapport avec les systèmes de DME couverts par son mandat;

f) mettre fin au mandat si le fabricant ne respecte pas les obligations qui lui incombent au titre du présent règlement;

g) s'assurer que la documentation technique visée à l'article 37 peut être mise à la disposition des autorités concernées, sur demande.

3. En cas de changement de mandataire, les modalités précises de ce changement portent au moins sur ce qui suit:

a) la date de fin du mandat du mandataire sortant et la date de début du mandat du nouveau mandataire;

b) les modalités de transfert des documents, y compris les questions de confidentialité et de droits de propriété.

4. Lorsque le fabricant est établi en dehors de l'Union et n'a pas respecté les obligations fixées à l'article 30, le mandataire est conjointement et solidairement responsable de la non-conformité au présent règlement au même titre que le fabricant.

Article 32

Obligations des importateurs

1. Les importateurs ne mettent sur le marché de l'Union que des systèmes de DME conformes aux exigences essentielles fixées à l'annexe II ainsi qu'aux spécifications communes visées à l'article 36.

2. Avant de mettre un système de DME à disposition sur le marché, les importateurs veillent à ce que:

a) le fabricant ait établi la documentation technique visée à l'article 37 et la déclaration UE de conformité;

b) le fabricant soit identifié et un mandataire ait été désigné conformément à l'article 31;

c) le système de DME porte le marquage CE de conformité visé à l'article 41 après que la procédure d'évaluation de la conformité a été achevée;

d) le système de DME soit accompagné de la fiche d'information visée à l'article 38 et d'une notice d'utilisation claire et complète, y compris pour son entretien, dans des formats accessibles.

3. Les importateurs indiquent, dans un document accompagnant le système de DME, leur nom, leur raison sociale ou leur marque déposée, l'adresse postale, le site internet, l'adresse électronique ou d'autres coordonnées numériques grâce auxquels ils peuvent être contactés. Les coordonnées indiquent un point unique auquel le fabricant peut être contacté et sont rédigées dans une langue qui peut être aisément comprise par les utilisateurs et les autorités de surveillance du marché. Les importateurs veillent à ce qu'aucune étiquette supplémentaire ne cache ou ne rende moins visibles les informations fournies par le fabricant qui apparaissent sur l'étiquette originale qui est fournie pour le système de DME.

4. Les importateurs veillent à ce que le système de DME, tant qu'il est sous leur responsabilité, ne soit pas modifié de telle sorte que sa conformité aux exigences essentielles fixées à l'annexe II et aux exigences éventuelles adoptées en vertu de l'article 42 soit compromise.

5. Lorsqu'un importateur considère ou a des raisons de croire qu'un système de DME n'est pas ou n'est plus conforme aux exigences essentielles fixées à l'annexe II et aux exigences éventuelles adoptées en vertu de l'article 42, il ne met pas le système de DME à disposition sur le marché, ou, si ce système de DME était déjà mis sur le marché, procède au rappel ou au retrait du système de DME jusqu'à sa mise en conformité. Dans le cas d'un rappel ou d'un retrait, l'importateur informe sans retard indu le fabricant de ce système de DME, les utilisateurs et les autorités de surveillance du marché de l'État membre dans lequel il a mis le système de DME à disposition sur le marché de ce rappel ou de ce retrait, en apportant notamment des précisions sur la non-conformité et sur toute mesure corrective prise.

Lorsqu'un importateur estime ou a des raisons de croire qu'un système de DME présente un risque pour la santé ou la sécurité des personnes physiques, il en informe sans retard indu les autorités de surveillance du marché de l'État membre dans lequel il est établi ainsi que le fabricant et, le cas échéant, le mandataire.

6. Les importateurs tiennent une copie de la déclaration UE de conformité à la disposition des autorités de surveillance du marché pendant la durée prévue à l'article 30, paragraphe 3, et veillent à ce que la documentation technique visée à l'article 37 puisse être mise à la disposition de ces autorités sur demande.

7. À la suite d'une demande motivée des autorités de surveillance du marché des États membres concernés, les importateurs communiquent à ces autorités toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système de DME. Les importateurs coopèrent avec ces autorités, à leur demande, et avec le fabricant et, le cas échéant, avec le mandataire dans une langue officielle de l'État membre dans lequel l'autorité de surveillance du marché est située. Les importateurs coopèrent avec ces autorités, à leur demande, en vue de prendre toute mesure permettant de mettre leurs systèmes de DME en conformité avec les exigences essentielles applicables aux composants logiciels harmonisés fixées à l'annexe II ou d'assurer le rappel ou le retrait des systèmes de DME qui ne sont pas conformes à ces exigences essentielles.

8. Les importateurs mettent en place des canaux de communication et veillent à ce que ces canaux soient accessibles pour permettre aux utilisateurs d'introduire des réclamations, et tiennent un registre des réclamations, des systèmes de DME non conformes et des rappels et retraits de systèmes de DME. Les importateurs vérifient que les canaux de réclamation mis en place en vertu de l'article 30, paragraphe 1, point n), sont à la disposition du public pour permettre aux utilisateurs d'introduire des réclamations et de recevoir toute communication concernant tout risque lié à leur santé ou à leur sécurité, ou concernant d'autres questions relatives à la protection de l'intérêt public, et permettre aux utilisateurs d'être informés de tout incident grave impliquant un système de DME. Lorsque de tels canaux de réclamation n'ont pas été mis en place, les importateurs les mettent en place et tiennent compte des besoins en matière d'accessibilité des groupes vulnérables et des personnes handicapées.

9. Les importateurs examinent les réclamations et assurent un suivi des informations qu'ils reçoivent concernant des incidents impliquant un système de DME qu'ils ont mis à disposition sur le marché. Les importateurs enregistrent ces réclamations, ainsi que tout rappel ou retrait de systèmes de DME et toute mesure corrective prise en vue de la mise en conformité du système de DME, dans le registre visé à l'article 30, paragraphe 1, point o), ou dans leur propre registre interne. Les importateurs tiennent le fabricant, les distributeurs et, le cas échéant, les mandataires informés en temps utile de l'examen et du suivi réalisés et de leur issue.

Article 33

Obligations des distributeurs

1. Avant de mettre un système de DME à disposition sur le marché, les distributeurs vérifient que:

a) le fabricant a rédigé la déclaration UE de conformité;

b) le système de DME porte le marquage CE de conformité;

c) le système de DME est accompagné de la fiche d'information visée à l'article 38 et d'une notice d'utilisation claire et complète dans des formats accessibles;

d) le cas échéant, l'importateur s'est conformé aux exigences énoncées à l'article 32, paragraphe 3.

2. Les distributeurs veillent à ce qu'un système de DME, tant qu'il est sous leur responsabilité, ne soit pas modifié de telle sorte que sa conformité aux exigences essentielles fixées à l'annexe II et aux exigences éventuelles adoptées en vertu de l'article 42 soit compromise.

3. Lorsqu'un distributeur estime ou a des raisons de croire qu'un système de DME n'est pas conforme aux exigences essentielles fixées à l'annexe II et aux exigences éventuelles adoptées en vertu de l'article 42, il ne met pas ledit système de DME à disposition sur le marché jusqu'à la mise en conformité dudit système. À cet effet, le distributeur informe sans retard indu le fabricant ou l'importateur ainsi que les autorités de surveillance du marché des États membres dans lesquels le système de DME a été mis à disposition sur le marché ou doit l'être. Lorsqu'un distributeur estime ou a des raisons de croire qu'un système de DME présente un risque pour la santé ou la sécurité des personnes physiques, il en informe les autorités de surveillance du marché de l'État membre dans lequel il est établi, ainsi que le fabricant et l'importateur.

4. Sur demande motivée d'une autorité de surveillance du marché, les distributeurs communiquent à cette autorité toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système de DME. Ils coopèrent avec cette autorité, à sa demande, et avec le fabricant, l'importateur et, le cas échéant, le mandataire du fabricant, en vue de prendre toute mesure permettant de mettre le système de DME en conformité avec les exigences essentielles fixées à l'annexe II et avec les exigences éventuelles adoptées en vertu de l'article 42 ou de le rappeler ou de le retirer.

Article 34

Cas dans lesquels les obligations des fabricants d'un système de DME s'appliquent à d'autres entités ou personnes

Un importateur, distributeur ou utilisateur est considéré comme un fabricant aux fins du présent règlement et est soumis aux obligations fixées à l'article 30 dans les cas suivants:

a) lorsqu'il met un système de DME à disposition sur le marché sous son propre nom ou sa propre marque commerciale;

b) lorsqu'il modifie un système de DME déjà mis sur le marché de telle sorte que la conformité aux exigences applicables pourrait être compromise; ou

c) lorsqu'il modifie un système de DME de telle sorte que cela entraîne des modifications de la destination déclarée par le fabricant.

Article 35

Identification des opérateurs économiques

Sur demande, les opérateurs économiques communiquent aux autorités de surveillance du marché, pendant une période de dix ans à compter de la date de mise sur le marché du dernier système de DME couvert par la déclaration UE de conformité, l'identité de:

a) tout opérateur économique qui leur a fourni un système de DME; et

b) tout opérateur économique auquel ils ont fourni un système de DME.

SECTION 3

Conformité des composants logiciels harmonisés des systèmes de DME

Article 36

Spécifications communes

1. Au plus tard le 26 mars 2027, la Commission adopte, par voie d'actes d'exécution, des spécifications communes en ce qui concerne les exigences essentielles fixées à l'annexe II, y compris un modèle commun et un délai pour la mise en œuvre de ces spécifications communes. Le cas échéant, ces spécifications communes tiennent compte des spécificités des dispositifs médicaux et des systèmes d'IA à haut risque visés à l'article 27, paragraphes 1 et 2, respectivement, y compris des normes les plus récentes applicables à l'informatique de la santé et du format européen d'échange des dossiers médicaux électroniques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Les spécifications communes visées au paragraphe 1 comprennent les informations et les éléments suivants:

a) leur champ d'application;

b) leur applicabilité aux différentes catégories de systèmes de DME ou aux fonctions qui y sont incluses;

c) leur version;

d) la période de validité;

e) une partie normative;

f) une partie explicative, comprenant les éventuelles lignes directrices pertinentes pour la mise en œuvre.

3. Les spécifications communes visées au paragraphe 1 peuvent englober des éléments ayant trait à ce qui suit:

a) aux ensembles de données contenant des données de santé électroniques et définissant des structures, telles que des champs de données et des groupes de données pour la représentation de contenu clinique et d'autres parties des données de santé électroniques;

b) aux systèmes de codage et aux valeurs à utiliser dans les ensembles de données contenant des données de santé électroniques, en tenant dûment compte à la fois de l'harmonisation future éventuelle des terminologies et de leur compatibilité avec les terminologies en vigueur au niveau national;

c) à d'autres exigences liées à la qualité des données, telles que l'exhaustivité et l'exactitude des données de santé électroniques;

d) aux spécifications techniques, normes et profils pour l'échange de données de santé électroniques;

e) aux exigences et principes concernant la sécurité des patients ainsi que la sécurité, la confidentialité, l'intégrité et la protection des données de santé électroniques;

f) aux spécifications et exigences relatives à la gestion de l'identification et à l'utilisation de l'identification électronique.

4. Les systèmes de DME, les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro et les systèmes d'IA à haut risque visés aux articles 25 et 27 qui sont conformes aux spécifications communes visées au paragraphe 1 du présent article sont considérés comme étant conformes aux exigences essentielles couvertes par ces spécifications communes ou par des parties de celles-ci, fixées à l'annexe II, et couverts par ces spécifications communes ou par les parties pertinentes de celles-ci.

5. Lorsque des spécifications communes couvrant les exigences d'interopérabilité et de sécurité des systèmes de DME ont une incidence sur des dispositifs médicaux, sur des dispositifs médicaux de diagnostic in vitro ou sur des systèmes d'IA à haut risque relevant d'autres actes juridiques, tels que le règlement (UE) 2017/745, (UE) 2017/746 ou (UE) 2024/1689, l'adoption de ces spécifications communes peut être précédée d'une consultation du groupe de coordination en matière de dispositifs médicaux (GCDM) institué par l'article 103 du règlement (UE) 2017/745 ou du Comité européen de l'intelligence artificielle créé par l'article 65 du règlement (UE) 2024/1689, et du comité européen de la protection des données, selon le cas.

6. Lorsque des spécifications communes couvrant les exigences d'interopérabilité et de sécurité des dispositifs médicaux, des dispositifs médicaux de diagnostic in vitro ou des systèmes d'IA à haut risque relevant d'autres actes juridiques, tels que le règlement (UE) 2017/745, (UE) 2017/746 ou (UE) 2024/1689, ont une incidence sur les systèmes de DME, la Commission veille à ce que l'adoption de ces spécifications communes soit précédée d'une consultation du comité de l'EEDS et du comité européen de la protection des données, selon le cas.

Article 37

Documentation technique

1. Les fabricants établissent une documentation technique avant la mise sur le marché ou la mise en service du système de DME et tiennent cette documentation à jour.

2. La documentation technique visée au paragraphe 1 du présent article démontre que le système de DME est conforme aux exigences essentielles fixées à l'annexe II et fournit aux autorités de surveillance du marché toutes les informations nécessaires pour évaluer la conformité du système de DME à ces exigences. Cette documentation technique contient, au minimum, les éléments énoncés à l'annexe III et une référence aux résultats obtenus dans un environnement d'essai numérique européen visé à l'article 40.

3. La documentation technique visée au paragraphe 1 est établie dans une langue officielle de l'État membre concerné ou dans une langue qui peut être aisément comprise dans ledit État membre. À la suite d'une demande motivée d'une autorité de surveillance du marché d'un État membre, le fabricant fournit une traduction des parties pertinentes de la documentation technique dans une langue officielle de cet État membre.

4. Lorsqu'une autorité de surveillance du marché demande à un fabricant la documentation technique ou une traduction de certaines parties de cette documentation, le fabricant fournit cette documentation technique ou cette traduction dans un délai de 30 jours à compter de la date de la demande, à moins qu'un délai plus court ne soit justifié en raison d'un risque sérieux et immédiat. Si le fabricant ne se conforme pas aux exigences des paragraphes 1, 2 et 3 du présent article, l'autorité de surveillance du marché peut exiger qu'un essai soit effectué par un organisme indépendant à ses frais dans un délai déterminé afin de vérifier la conformité aux exigences essentielles fixées à l'annexe II ainsi qu'aux spécifications communes visées à l'article 36.

Article 38

Fiche d'information accompagnant le système de DME

1. Les systèmes de DME sont accompagnés d'une fiche d'information, contenant des informations concises, complètes, exactes et claires, qui sont pertinentes, accessibles et compréhensibles pour les utilisateurs professionnels.

2. La fiche d'information visée au paragraphe 1 indique:

a) l'identité, la raison sociale ou la marque déposée et les coordonnées du fabricant ainsi que, le cas échéant, de son mandataire;

b) le nom et la version du système de DME et la date de sa mise en service;

c) la destination du système de DME;

d) les catégories de données de santé électroniques pour le traitement desquelles le système de DME a été conçu;

e) les normes, formats et spécifications soutenus par le système de DME, ainsi que les versions de ces normes, formats et spécifications.

3. Au lieu de fournir la fiche d'information visée au paragraphe 1 du présent article avec le système de DME, les fabricants peuvent introduire les informations visées au paragraphe 2 du présent article dans la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être visée à l'article 49.

Article 39

Déclaration UE de conformité

1. La déclaration UE de conformité visée à l'article 30, paragraphe 1, point e), atteste que le fabricant d'un système de DME a démontré que les exigences essentielles fixées à l'annexe II ont été remplies.

2. Lorsqu'un système de DME fait l'objet d'autres actes juridiques de l'Union en ce qui concerne des aspects qui ne sont pas couverts par le présent règlement, qui imposent aussi une déclaration UE de conformité du fabricant attestant qu'il a été démontré que les exigences prévues dans ces actes juridiques ont été remplies, une seule déclaration UE de conformité est établie pour tous les actes juridiques de l'Union applicables au système de DME. La déclaration UE de conformité contient toutes les informations nécessaires à l'identification des actes juridiques de l'Union auxquels la déclaration se rapporte.

3. La déclaration UE de conformité contient les informations qui figurent à l'annexe IV et est traduite dans une ou plusieurs des langues officielles de l'Union déterminées par les États membres dans lesquels le système de DME est mis à disposition.

4. Lorsqu'une déclaration UE de conformité est établie dans un format numérique, elle est rendue accessible en ligne pendant la durée de vie prévue du système de DME et, en tout état de cause, pendant au moins dix ans à compter de la mise sur le marché ou de la mise en service du système de DME.

5. En établissant la déclaration UE de conformité, le fabricant assume la responsabilité de la conformité des composants logiciels harmonisés du système de DME aux exigences fixées dans le présent règlement lorsque le système de DME est mis sur le marché ou mis en service.

6. La Commission publie un modèle uniforme standard de déclaration UE de conformité, qu'elle met à disposition dans un format numérique dans toutes les langues officielles de l'Union.

Article 40

Environnement d'essai numérique européen

1. La Commission élabore un environnement d'essai numérique européen pour l'évaluation des composants logiciels harmonisés des systèmes de DME. La Commission met à disposition le logiciel permettant l'exploitation de l'environnement d'essai numérique européen sous la forme d'un code source ouvert.

2. Les États membres gèrent des environnements d'essai numériques pour l'évaluation des composants logiciels harmonisés des systèmes de DME. Ces environnements d'essai numériques sont conformes aux spécifications communes applicables à l'environnement d'essai numérique européen établies en vertu du paragraphe 4. Les États membres informent la Commission des environnements d'essai numériques dont ils disposent.

3. Avant la mise sur le marché de systèmes de DME, les fabricants utilisent les environnements d'essai numériques visés aux paragraphes 1 et 2 du présent article pour évaluer les composants logiciels harmonisés des systèmes de DME. Les résultats de cette évaluation sont intégrés à la documentation visée à l'article 37. Les éléments pour lesquels les résultats de l'évaluation sont positifs sont présumés être conformes au présent règlement.

4. La Commission établit, par voie d'actes d'exécution, les spécifications communes applicables à l'environnement d'essai numérique européen. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 41

Marquage CE de conformité

1. Le marquage CE de conformité est apposé de manière visible, lisible et indélébile sur les documents d'accompagnement du système de DME et, le cas échéant, sur l'emballage du système de DME.

2. Le marquage CE de conformité est apposé avant la mise sur le marché du système de DME.

3. Le marquage CE de conformité est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) nº 765/2008.

Article 42

Exigences nationales et rapports à la Commission

1. Les États membres peuvent adopter des exigences nationales applicables aux systèmes de DME et des dispositions relatives à leur évaluation de la conformité en ce qui concerne des aspects autres que les composants logiciels harmonisés des systèmes de DME.

2. Les exigences ou dispositions nationales visées au paragraphe 1 ne peuvent avoir d'effets négatifs sur les composants logiciels harmonisés des systèmes de DME.

3. Lorsque les États membres adoptent des exigences ou des dispositions conformément au paragraphe 1, ils en informent la Commission.

SECTION 4

Surveillance du marché des systèmes de DME

Article 43

Autorités de surveillance du marché

1. Le règlement (UE) 2019/1020 s'applique aux systèmes de DME en ce qui concerne les exigences applicables aux systèmes de DME couverts par le présent chapitre et les risques présentés par ces systèmes.

2. Les États membres désignent l'autorité de surveillance du marché ou les autorités de surveillance du marché chargées de la mise en œuvre du présent chapitre. Ils dotent leurs autorités de surveillance du marché des pouvoirs nécessaires ainsi que des ressources humaines, financières et techniques, de l'équipement et des connaissances nécessaires pour accomplir correctement les tâches qui leur incombent en vertu du présent règlement. Les autorités de surveillance du marché sont habilitées à prendre les mesures de surveillance du marché visées à l'article 16 du règlement (UE) 2019/1020 pour faire respecter les obligations fixées au présent chapitre. Les États membres communiquent l'identité des autorités de surveillance du marché qu'ils désignent à la Commission. La Commission et les États membres mettent ces informations à la disposition du public.

3. Les autorités de surveillance du marché désignées en application du paragraphe 2 du présent article peuvent être les mêmes autorités que les autorités de santé numérique désignées en application de l'article 19. Lorsqu'une autorité de santé numérique exécute des tâches d'une autorité de surveillance du marché, les États membres veillent à éviter tout conflit d'intérêts.

4. Les autorités de surveillance du marché communiquent une fois par an à la Commission les résultats des activités de surveillance du marché pertinentes.

5. Lorsqu'un fabricant ou un autre opérateur économique ne coopère pas avec une autorité de surveillance du marché ou lorsque les informations et la documentation qu'il a fournies sont incomplètes ou incorrectes, l'autorité de surveillance du marché peut prendre toutes les mesures appropriées pour interdire ou limiter la mise à disposition sur le marché du système de DME concerné jusqu'à ce que le fabricant ou l'opérateur économique concerné coopère ou fournisse des informations complètes et correctes, ou jusqu'à ce qu'il procède au rappel ou au retrait dudit système de DME du marché.

6. Les autorités de surveillance du marché des États membres coopèrent entre elles ainsi qu'avec la Commission. La Commission facilite l'organisation des échanges d'informations nécessaires à cette coopération.

7. Pour les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro ou les systèmes d'IA à haut risque visés à l'article 27, paragraphes 1 et 2, les autorités responsables de la surveillance du marché sont celles visées à l'article 93 du règlement (UE) 2017/745, à l'article 88 du règlement (UE) 2017/746 ou à l'article 70 du règlement (UE) 2024/1689, selon le cas.

Article 44

Gestion des risques présentés par les systèmes de DME et des incidents graves

1. Lorsqu'une autorité de surveillance du marché d'un État membre a des raisons de croire qu'un système de DME présente un risque pour la santé, la sécurité ou les droits des personnes physiques ou pour la protection des données à caractère personnel, elle procède à une évaluation du système de DME concerné couvrant toutes les exigences pertinentes prévues par le présent règlement. Le fabricant, le mandataire du fabricant et tous les autres opérateurs économiques concernés coopèrent à cette fin avec l'autorité de surveillance du marché, en tant que de besoin, et prennent toutes les mesures appropriées pour faire en sorte que le système de DME concerné ne présente plus ce risque lors de sa mise sur le marché, ou pour procéder au rappel ou au retrait du système de DME du marché dans un délai raisonnable.

2. Lorsque les autorités de surveillance du marché d'un État membre considèrent que la non-conformité du système de DME n'est pas limitée à leur territoire national, elles informent la Commission et les autorités de surveillance du marché des autres États membres des résultats de l'évaluation visée au paragraphe 1 du présent article et des mesures correctives qu'elles ont enjoint à l'opérateur économique de prendre en vertu de l'article 16, paragraphe 2, du règlement (UE) 2019/1020.

3. Lorsqu'une autorité de surveillance du marché constate qu'un système de DME a porté préjudice à la santé ou à la sécurité de personnes physiques, ou à certains aspects de la protection de l'intérêt public, le fabricant fournit immédiatement des informations et une documentation, selon le cas, à la personne physique ou à l'utilisateur affectés, et, le cas échéant, aux autres tiers affectés par ledit préjudice, sans préjudice des règles en matière de protection des données.

4. L'opérateur économique concerné visé au paragraphe 1 s'assure que des mesures correctives sont prises à l'égard de tous les systèmes de DME concernés qu'il a mis sur le marché dans toute l'Union.

5. L'autorité de surveillance du marché informe sans retard indu la Commission et les autorités de surveillance du marché, ou, le cas échéant, les autorités de contrôle au titre du règlement (UE) 2016/679, d'autres États membres des mesures correctives visées au paragraphe 2. Cette information comprend toutes les précisions disponibles, notamment les données nécessaires à l'identification du système de DME concerné, l'origine et la chaîne d'approvisionnement du système de DME, la nature du risque encouru, ainsi que la nature et la durée des mesures nationales prises.

6. Lorsqu'une constatation faite par une autorité de surveillance du marché ou un incident grave porté à la connaissance de cette autorité concerne la protection de données à caractère personnel, ladite autorité de surveillance du marché en informe sans retard indu les autorités de contrôle compétentes au titre du règlement (UE) 2016/679 et coopère avec elles.

7. Les fabricants de systèmes de DME mis sur le marché ou mis en service signalent tout incident grave impliquant un système de DME aux autorités de surveillance du marché des États membres dans lesquels l'incident grave s'est produit et des États membres dans lesquels ces systèmes de DME sont mis sur le marché ou mis en service. Ce signalement contient également une description des mesures correctives prises ou envisagées par le fabricant. Les États membres peuvent prévoir que les utilisateurs de systèmes de DME mis sur le marché ou mis en service peuvent signaler ces incidents.

Le signalement requis en vertu du premier alinéa du présent paragraphe est effectué, sans préjudice des exigences en matière de notification des incidents établies dans la directive (UE) 2022/2555, immédiatement après que le fabricant a établi un lien de causalité, ou la probabilité raisonnable qu'un tel lien existe, entre le système de DME et l'incident grave et, en tout état de cause, au plus tard trois jours après que le fabricant a eu connaissance de l'incident grave impliquant le système de DME.

8. Les autorités de surveillance du marché visées au paragraphe 7 informent, sans retard, les autres autorités de surveillance du marché de l'incident grave et des mesures correctives prises ou envisagées par le fabricant, ou exigées de celui-ci, pour réduire au minimum le risque de répétition de l'incident grave.

9. Lorsque les tâches de l'autorité de surveillance du marché ne sont pas exécutées par l'autorité de santé numérique, l'autorité de surveillance du marché coopère avec l'autorité de santé numérique. L'autorité de surveillance du marché informe l'autorité de santé numérique de tout incident grave, des systèmes de DME présentant un risque, y compris des risques en matière d'interopérabilité, de sécurité des patients et de sûreté, de toute mesure corrective et de tout rappel ou de tout retrait de tels systèmes de DME.

10. Pour les incidents mettant en péril la sécurité des patients ou la sécurité de l'information, les autorités de surveillance du marché peuvent prendre des mesures immédiates et exiger du fabricant du système de DME concerné, de son mandataire et d'autres opérateurs économiques, le cas échéant, qu'ils prennent des mesures correctives immédiates.

Article 45

Traitement des cas de non-conformité

1. Lorsqu'une autorité de surveillance du marché constate un cas de non-conformité, elle requiert du fabricant du système de DME concerné, de son mandataire et de tous les autres opérateurs économiques concernés qu'ils prennent, dans un délai déterminé, les mesures correctives appropriées en vue de la mise en conformité du système de DME. Ces constats de non-conformité incluent les cas suivants, sans s'y limiter:

a) le système de DME n'est pas conforme aux exigences essentielles fixées à l'annexe II ou aux spécifications communes visées à l'article 36;

b) la documentation technique n'est pas disponible, est incomplète ou n'est pas conforme à l'article 37;

c) la déclaration UE de conformité n'a pas été établie ou n'a pas été établie correctement conformément à l'article 39;

d) le marquage CE de conformité a été apposé en violation de l'article 41 ou n'a pas été apposé;

e) les obligations d'enregistrement prévues à l'article 49 n'ont pas été remplies.

2. Lorsque le fabricant du système de DME concerné, son mandataire ou tout autre opérateur économique concerné ne prend pas de mesures correctives appropriées dans un délai raisonnable, les autorités de surveillance du marché prennent toutes les mesures provisoires appropriées pour interdire ou limiter la mise à disposition du système de DME sur le marché de leurs États membres ou pour procéder au rappel ou au retrait du système de DME de ce marché.

Les autorités de surveillance du marché informent, sans retard, la Commission et les autorités de surveillance du marché des autres États membres de ces mesures provisoires. Ces informations contiennent toutes les précisions disponibles, notamment les données nécessaires pour identifier le système de DME non conforme, son origine, la nature de la non-conformité alléguée et le risque encouru, ainsi que la nature et la durée des mesures prises par les autorités de surveillance du marché et les arguments avancés par l'opérateur économique concerné. En particulier, les autorités de surveillance du marché indiquent si la non-conformité découle de l'une des causes suivantes:

a) le non-respect par le système de DME des exigences essentielles fixées à l'annexe II;

b) des lacunes en ce qui concerne les spécifications communes visées à l'article 36.

3. Les autorités de surveillance du marché autres que celles qui ont entamé la procédure en vertu du présent article informent, sans retard, la Commission et les autorités de surveillance du marché des autres États membres de toute mesure adoptée, de toute information supplémentaire dont elles disposent à propos de la non-conformité du système de DME concerné et, dans l'éventualité où elles s'opposeraient à la mesure nationale adoptée, de leurs objections.

4. Lorsque, dans les trois mois à compter de la réception des informations visées au paragraphe 2, deuxième alinéa, aucune objection n'a été soulevée soit par une autorité de surveillance du marché d'un autre État membre soit par la Commission à l'encontre d'une mesure provisoire prise par une autorité de surveillance du marché, cette mesure est réputée justifiée.

5. Lorsque la non-conformité visée au paragraphe 1 persiste, l'autorité de surveillance du marché concernée prend toutes les mesures appropriées pour interdire ou limiter la mise à disposition du système de DME sur le marché ou pour procéder au rappel ou au retrait du système de DME du marché.

Article 46

Procédure de sauvegarde de l'Union

1. Lorsque, dans le cadre de l'article 44, paragraphe 2, et de l'article 45, paragraphe 3, des objections sont soulevées à l'égard d'une mesure nationale prise par une autorité de surveillance du marché, ou lorsque la Commission considère qu'une mesure nationale est contraire au droit de l'Union, la Commission entreprend sans tarder des consultations avec cette autorité de surveillance du marché et les opérateurs économiques concernés et procède à l'évaluation de la mesure nationale concernée. Sur la base des résultats de cette évaluation, la Commission adopte une décision d'exécution déterminant si la mesure nationale est justifiée. Cette décision d'exécution est adoptée en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2. La Commission adresse sa décision d'exécution à tous les États membres et la communique immédiatement à ceux-ci ainsi qu'aux opérateurs économiques concernés.

2. Si la Commission considère que la mesure nationale visée au paragraphe 1 est justifiée, tous les États membres concernés prennent les mesures nécessaires pour procéder au retrait du système de DME non conforme de leur marché, et en informent la Commission.

Si la Commission considère que la mesure nationale visée au paragraphe 1 n'est pas justifiée, l'État membre concerné révoque cette mesure.

SECTION 5

Autres dispositions relatives à l'interopérabilité

Article 47

Labellisation des applications de bien-être

1. Lorsque le fabricant d'une application de bien-être allègue l'interopérabilité de cette application avec un système de DME en ce qui concerne les composants logiciels harmonisés des systèmes de DME et, par conséquent, sa conformité aux spécifications communes visées à l'article 36 et aux exigences essentielles fixées à l'annexe II, l'application de bien-être est accompagnée d'un label indiquant clairement sa conformité auxdites spécifications et exigences. Ce label est délivré par le fabricant de l'application de bien-être.

2. Les informations suivantes doivent figurer sur le label visé au paragraphe 1:

a) les catégories de données de santé électroniques pour lesquelles la conformité aux exigences essentielles fixées à l'annexe II a été confirmée;

b) une référence aux spécifications communes pour démontrer la conformité;

c) la durée de validité du label.

3. La Commission détermine, par voie d'actes d'exécution, le format et le contenu du label visé au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

4. Le label est rédigé dans une ou plusieurs langues officielles de l'Union ou dans une langue qui peut être aisément comprise, déterminée par l'État membre dans lequel l'application de bien-être est mise sur le marché ou mise en service.

5. La durée de validité du label ne dépasse pas trois ans.

6. Si l'application de bien-être fait partie intégrante d'un dispositif ou est intégrée dans un dispositif après sa mise en service, le label qui l'accompagne figure dans l'application elle-même ou il est apposé sur ce dispositif. Lorsque l'application de bien-être consiste seulement en un logiciel, le label a un format numérique et figure dans l'application elle-même. Le label peut également être apposé sous la forme d'un code-barre à deux dimensions (2D).

7. Les autorités de surveillance du marché vérifient la conformité des applications de bien-être aux exigences essentielles fixées à l'annexe II.

8. Chaque fournisseur d'une application de bien-être pour laquelle un label a été délivré veille à ce que l'application de bien-être qui est mise sur le marché ou mise en service soit accompagnée du label pour chaque unité individuelle, gratuitement.

9. Chaque distributeur d'une application de bien-être pour laquelle un label a été délivré met le label à la disposition des clients au point de vente sous format électronique.

Article 48

Interopérabilité des applications de bien-être avec les systèmes de DME

1. Les fabricants d'applications de bien-être peuvent alléguer l'interopérabilité de ces applications avec un système de DME à condition de satisfaire aux spécifications communes et aux exigences essentielles visées, respectivement, à l'article 36 et à l'annexe II. Dans le cas d'une telle allégation, ces fabricants informent dûment les utilisateurs de l'interopérabilité de ces applications de bien-être et des effets d'une telle interopérabilité.

2. L'interopérabilité des applications de bien-être avec les systèmes de DME n'implique pas le partage automatique avec le système de DME, ou la transmission automatique à ce dernier, de tout ou partie des données de santé issues de l'application de bien-être. Le partage ou la transmission de ces données n'est possible que s'il a lieu conformément à l'article 5 et qu'après que la personne physique concernée a donné son consentement et l'interopérabilité est exclusivement limitée à ces fins. Les fabricants d'applications de bien-être qui allèguent l'interopérabilité de ces applications avec un système de DME veillent à ce que la personne physique concernée soit en mesure de choisir les catégories de données de santé issues de l'application de bien-être qui doivent être intégrées au système de DME et les conditions du partage ou de la transmission de ces catégories de données.

SECTION 6

Enregistrement des systèmes de DME et des applications de bien-être

Article 49

Base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être

1. La Commission établit et tient à jour une base de données de l'Union européenne accessible au public contenant des données sur les systèmes de DME pour lesquels une déclaration UE de conformité a été délivrée en vertu de l'article 39 et sur les applications de bien-être pour lesquelles un label a été délivré en vertu de l'article 47 (ci-après dénommée «base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être»).

2. Avant la mise sur le marché ou la mise en service d'un système de DME visé à l'article 26 ou d'une application de bien-être visée à l'article 47, le fabricant du système de DME ou de l'application de bien-être, ou, le cas échéant, son mandataire, introduit les données requises visées au paragraphe 4 du présent article dans la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être, y compris, dans le cas des systèmes de DME, les résultats de l'évaluation visée à l'article 40.

3. Les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro ou les systèmes d'IA à haut risque visés à l'article 27, paragraphes 1 et 2, du présent règlement sont également enregistrés dans les bases de données établies en application du règlement (UE) 2017/745, (UE) 2017/746 ou (UE) 2024/1689, selon le cas. Dans ces cas, les données à introduire sont également transmises à la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour compléter le présent règlement en déterminant la liste des données requises que les fabricants de systèmes de DME et d'applications de bien-être doivent introduire dans la base de données de l'Union européenne pour l'enregistrement des systèmes de DME et des applications de bien-être en vertu du paragraphe 2 du présent article.

CHAPITRE IV

UTILISATION SECONDAIRE

SECTION 1

Conditions générales relatives à l'utilisation secondaire

Article 50

Applicabilité aux détenteurs de données de santé

1. Les catégories de détenteurs de données de santé suivantes sont exemptées des obligations qui incombent aux détenteurs de données de santé fixées dans le présent chapitre:

a) les personnes physiques, y compris les chercheurs individuels;

b) les personnes morales qui peuvent être qualifiées de microentreprises telles qu'elles sont définies à l'article 2, paragraphe 3, de l'annexe de la recommandation 2003/361/CE.

2. Les États membres peuvent prévoir dans leur droit national que les obligations des détenteurs de données de santé fixées dans le présent chapitre s'appliquent aux détenteurs de données de santé visés au paragraphe 1 qui relèvent de leur compétence.

3. Les États membres peuvent prévoir dans leur droit national que les entités d'intermédiation de données de santé s'acquittent des obligations de certaines catégories de détenteurs de données de santé. Dans ce cas, les données sont néanmoins considérées comme étant mises à disposition par plusieurs détenteurs de données de santé.

4. Les États membres notifient à la Commission les dispositions de droit national visées aux paragraphes 2 et 3 au plus tard le 26 mars 2029. Toute disposition légale ultérieure ou toute modification ultérieure d'une telle disposition est notifiée sans retard à la Commission.

Article 51

Catégories minimales de données de santé électroniques à des fins d'utilisation secondaire

1. Les détenteurs de données de santé mettent à disposition à des fins d'utilisation secondaire conformément au présent chapitre les catégories de données de santé électroniques ci-après:

a) les données de santé électroniques provenant de DME;

b) les données sur les facteurs ayant une incidence sur la santé, dont les déterminants socio-économiques, environnementaux et comportementaux de la santé;

c) les données agrégées sur les besoins en soins de santé, les ressources allouées aux soins de santé, la fourniture et l'accès en matière de soins de santé, les dépenses et le financement en matière de soins de santé;

d) les données sur les pathogènes ayant une incidence sur la santé humaine;

e) les données administratives liées aux soins de santé, dont les données relatives aux dispensations, aux demandes de remboursement et aux remboursements;

f) les données génétiques, épigénomiques et génomiques humaines;

g) d'autres données moléculaires humaines telles que les données protéomiques, transcriptomiques, métabolomiques, lipidomiques et d'autres données omiques;

h) les données de santé électroniques à caractère personnel générées automatiquement grâce aux dispositifs médicaux;

i) les données provenant d'applications de bien-être;

j) les données relatives au statut professionnel, ainsi qu'à la spécialisation et à l'établissement des professionnels de la santé intervenant dans le traitement d'une personne physique;

k) les données provenant des registres de données de santé basées sur la population, tels que les registres de santé publique;

l) les données contenues dans les registres médicaux et les registres de mortalité;

m) les données provenant d'essais cliniques, d'études cliniques, d'investigations cliniques et d'études de performance soumis au règlement (UE) nº 536/2014, au règlement (UE) 2024/1938 du Parlement européen et du Conseil ([35]), au règlement (UE) 2017/745 et au règlement (UE) 2017/746;

n) d'autres données de santé provenant de dispositifs médicaux;

o) les données provenant des registres de médicaments et des dispositifs médicaux;

p) les données provenant de cohortes de recherche, de questionnaires et d'enquêtes dans le domaine de la santé, après la première publication des résultats y afférents;

q) les données de santé provenant de biobanques et de bases de données associées.

2. Les États membres peuvent prévoir, dans leur droit national, que des catégories de données de santé électroniques supplémentaires sont mises à disposition à des fins d'utilisation secondaire en application du présent règlement.

3. Les États membres peuvent établir des règles relatives au traitement et à l'utilisation des données de santé électroniques contenant des améliorations liées au traitement de ces données, telles que des corrections, des annotations ou des enrichissements, sur la base d'une autorisation de traitement de données en vertu de l'article 68.

4. Les États membres peuvent introduire des mesures plus strictes et des garanties supplémentaires au niveau national visant à préserver le caractère sensible et la valeur des données relevant du paragraphe 1, points f), g), i) et q). Les États membres notifient, sans retard, ces mesures et garanties à la Commission ainsi que toute modification ultérieure les concernant.

Article 52

Droits de propriété intellectuelle et secrets d'affaires

1. Les données de santé électroniques protégées par des droits de propriété intellectuelle, des secrets d'affaires ou relevant du droit à la protection réglementaire des données prévue à l'article 10, paragraphe 1, de la directive 2001/83/CE du Parlement européen et du Conseil ([36]) ou à l'article 14, paragraphe 11, du règlement (CE) nº 726/2004 du Parlement européen et du Conseil ([37]) sont mises à disposition à des fins d'utilisation secondaire conformément aux règles fixées dans le présent règlement.

2. Les détenteurs de données de santé communiquent à l'organisme responsable de l'accès aux données de santé les données de santé électroniques comportant des contenus ou des informations protégés par des droits de propriété intellectuelle ou des secrets d'affaires ou couverts par le droit à la protection réglementaire des données prévu à l'article 10, paragraphe 1, de la directive 2001/83/CE ou à l'article 14, paragraphe 11, du règlement (CE) nº 726/2004. Les détenteurs

([35]) Règlement (UE) 2024/1938 du Parlement européen et du Conseil du 13 juin 2024 concernant les normes de qualité et de sécurité des substances d'origine humaine destinées à une application humaine et abrogeant les directives 2002/98/CE et 2004/23/CE (JO L, 2024/1938, 17.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1938/oj).

([36]) Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain (JO L 311 du 28.11.2001, p. 67).

([37]) Règlement (CE) nº 726/2004 du Parlement européen et du Conseil du 31 mars 2004 établissant des procédures de l'Union pour l'autorisation et la surveillance des médicaments à usage humain et instituant une Agence européenne des médicaments (JO L 136 du 30.4.2004, p. 1).

de données de santé déterminent quelles parties des ensembles de données sont concernées et justifient la nécessité de la protection spécifique des données. Les détenteurs de données de santé fournissent ces informations lorsqu'ils communiquent à l'organisme responsable de l'accès aux données de santé la description de l'ensemble de données qu'ils détiennent en vertu de l'article 60, paragraphe 3, du présent règlement, ou, au plus tard, après avoir reçu une demande de l'organisme responsable de l'accès aux données de santé.

3. Les organismes responsables de l'accès aux données de santé prennent toutes les mesures spécifiques appropriées et proportionnées, y compris de nature juridique, organisationnelle et technique, qu'ils jugent nécessaires pour protéger les droits de propriété intellectuelle, les secrets d'affaires ou le droit à la protection réglementaire des données prévu à l'article 10, paragraphe 1, de la directive 2001/83/CE ou à l'article 14, paragraphe 11, du règlement (CE) nº 726/2004. Les organismes responsables de l'accès aux données de santé demeurent responsables pour déterminer si ces mesures sont nécessaires et appropriées.

4. Lorsqu'ils délivrent des autorisations de traitement de données conformément à l'article 68, les organismes responsables de l'accès aux données de santé peuvent subordonner l'accès à certaines données de santé électroniques à des mesures juridiques, organisationnelles et techniques, qui peuvent comprendre des accords contractuels entre des détenteurs de données de santé et des utilisateurs de données de santé sur le partage de données comportant des informations ou des contenus protégés par des droits de propriété intellectuelle ou des secrets d'affaires. La Commission élabore et recommande des modèles non contraignants de clauses contractuelles applicables à ces accords.

5. Lorsque l'octroi d'un accès à des données de santé électroniques à des fins d'utilisation secondaire entraîne un risque grave de violation des droits de propriété intellectuelle, des secrets d'affaires ou du droit à la protection réglementaire des données prévu à l'article 10, paragraphe 1, de la directive 2001/83/CE ou à l'article 14, paragraphe 11, du règlement (CE) nº 726/2004, auquel il ne peut être remédié de manière satisfaisante, l'organisme responsable de l'accès aux données de santé refuse l'accès à ces données au demandeur de données de santé. L'organisme responsable de l'accès aux données de santé informe le demandeur de données de santé de ce refus et lui fournit une justification de ce refus. Les détenteurs de données de santé et les demandeurs de données de santé ont le droit d'introduire une réclamation conformément à l'article 81 du présent règlement.

Article 53

Finalités pour lesquelles des données de santé électroniques peuvent être traitées à des fins d'utilisation secondaire

1. Les organismes responsables de l'accès aux données de santé n'octroient l'accès aux données de santé électroniques visées à l'article 51 à des fins d'utilisation secondaire à un utilisateur de données de santé que lorsque le traitement des données par ledit utilisateur de données est nécessaire à l'une des finalités suivantes:

a) l'intérêt public dans le domaine de la santé publique ou de la santé au travail, telles que des activités destinées à la protection contre les menaces transfrontières graves pour la santé et à la surveillance de la santé publique ou des activités destinées à garantir un niveau élevé de qualité et de sécurité des soins de santé, y compris de sécurité des patients, et des médicaments ou des dispositifs médicaux;

b) l'élaboration de politiques et les activités réglementaires destinées à aider les organismes du secteur public ou les institutions, organes et organismes de l'Union, dont les autorités réglementaires, dans le secteur de la santé ou des soins, à accomplir les tâches définies dans leur mandat;

c) des statistiques, telles qu'elles sont définies à l'article 3, point 1), du règlement (CE) nº 223/2009, telles que les statistiques officielles aux échelons national, plurinational et de l'Union, en rapport avec les secteurs de la santé ou des soins;

d) des activités d'éducation ou d'enseignement dans les secteurs de la santé ou des soins au niveau de l'enseignement professionnel ou supérieur;

e) la recherche scientifique ayant trait aux secteurs de la santé ou des soins qui contribue à la santé publique ou aux évaluations des technologies de la santé, ou qui garantit un niveau élevé de qualité et de sécurité des soins de santé, des médicaments ou des dispositifs médicaux, dans le but d'en faire bénéficier les utilisateurs finals, tels que les patients, les professionnels de la santé et les administrateurs des services de santé, y compris:

   i) les activités de développement et d'innovation pour les produits ou services;

   ii) la formation, les essais et l'évaluation d'algorithmes, notamment dans les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro, les systèmes d'IA et les applications de santé numérique;

f) l'amélioration de la fourniture de soins, de l'optimisation des traitements et de la fourniture de soins de santé, sur la base des données de santé électroniques d'autres personnes physiques.

2. L'accès aux données de santé électroniques pour les finalités visées au paragraphe 1, points a), b) et c), est réservé aux organismes du secteur public et aux institutions, organes et organismes de l'Union exécutant des tâches qui leur ont été conférées par le droit de l'Union ou le droit national, y compris lorsque le traitement de données aux fins de l'accomplissement de ces tâches est effectué par un tiers pour le compte de ces organismes du secteur public ou d'institutions, organes et organismes de l'Union.

Article 54

Utilisation secondaire interdite

Les utilisateurs de données de santé ne traitent les données de santé électroniques à des fins d'utilisation secondaire que sur la base des finalités contenues dans une autorisation de traitement de données délivrée en vertu de l'article 68, dans une demande de données de santé approuvée en vertu de l'article 69 ou, dans les situations visées à l'article 67, paragraphe 3, dans une approbation d'accès émanant du participant autorisé à DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75 concerné, et conformément à ces finalités.

Il est, en particulier, interdit de demander l'accès aux données de santé électroniques obtenues moyennant une autorisation de traitement de données délivrée en vertu de l'article 68 ou une demande de données de santé approuvée en vertu de l'article 69, et de traiter de telles données, aux fins des utilisations suivantes:

a) une prise de décisions préjudiciables à une personne physique ou un groupe de personnes physiques sur la base de leurs données de santé électroniques; pour être qualifiées de «décisions» aux fins du présent point, celles-ci doivent produire des effets juridiques, sociaux ou économiques, ou avoir, de manière similaire, une incidence significative sur ces personnes physiques;

b) une prise de décisions, à l'égard d'une personne physique ou d'un groupe de personnes physiques, relatives à des offres d'emploi, proposant des conditions moins favorables dans le cadre de la fourniture de biens ou de services, y compris l'exclusion de ces personnes ou groupes du bénéfice d'un contrat d'assurance ou de crédit ou la modification de leurs cotisations et de leurs primes d'assurance ou de leurs conditions de prêt, ou la prise de toute autre décision, à l'égard d'une personne physique ou d'un groupe de personnes physiques, dont il découle une discrimination à leur encontre sur la base des données de santé obtenues;

c) l'exercice d'activités de publicité ou de marketing;

d) une mise au point de produits ou de services susceptibles de porter préjudice aux personnes, à la santé publique ou à la société au sens large, tels que les drogues illicites, les boissons alcoolisées, les produits du tabac et à base de nicotine, les armes ou les produits ou services qui sont conçus ou modifiés de sorte à créer une dépendance, à porter atteinte à l'ordre public ou à induire un risque pour la santé humaine;

e) l'exercice d'activités contraires aux dispositions éthiques fixées dans le droit national.

SECTION 2

Gouvernance et mécanismes pour l'utilisation secondaire

Article 55

Organismes responsables de l'accès aux données de santé

1. Les États membres désignent un ou plusieurs organismes responsables de l'accès aux données de santé chargés d'accomplir les tâches et de s'acquitter des obligations énoncées aux articles 57, 58 et 59. Les États membres peuvent soit créer un ou plusieurs nouveaux organismes du secteur public, soit s'appuyer sur des organismes du secteur public existants ou sur des services internes d'organismes du secteur public qui remplissent les conditions énoncées dans le présent article. Les tâches énoncées à l'article 57 peuvent être réparties entre différents organismes responsables de l'accès aux données de santé. Lorsqu'un État membre désigne plusieurs organismes responsables de l'accès aux données de santé, il désigne un organisme responsable de l'accès aux données de santé comme coordonnateur, chargé d'assurer la coordination des tâches avec les autres organismes responsables de l'accès aux données de santé tant sur le territoire dudit État membre que dans d'autres États membres.

Chaque organisme responsable de l'accès aux données de santé contribue à l'application cohérente du présent règlement dans l'ensemble de l'Union. À cette fin, les organismes responsables de l'accès aux données de santé coopèrent entre eux, avec la Commission et, en ce qui concerne les questions relatives à la protection des données, avec les autorités de contrôle compétentes.

2. Afin de soutenir les organismes responsables de l'accès aux données de santé dans l'accomplissement efficace de leurs tâches et dans l'exercice de leurs pouvoirs, les États membres veillent à ce que chaque organisme responsable de l'accès aux données de santé dispose des éléments suivants:

a) les ressources humaines, financières et techniques nécessaires;

b) l'expertise nécessaire; et

c) les locaux et les infrastructures nécessaires.

Lorsqu'une évaluation par des organismes chargés des questions d'éthique est requise en vertu du droit national, ces organismes mettent leur expertise à la disposition de l'organisme responsable de l'accès aux données de santé. À titre d'alternative, les États membres peuvent prévoir que les organismes chargés des questions d'éthique font partie de l'organisme responsable de l'accès aux données de santé.

3. Les États membres veillent à éviter tout conflit d'intérêts entre les services des organismes responsables de l'accès aux données de santé réalisant les différentes tâches de ces organismes, en prévoyant, par exemple, des garanties organisationnelles telles que la séparation des différentes fonctions des organismes responsables de l'accès aux données de santé, y compris l'évaluation des demandes, la réception et la préparation d'ensembles de données, par exemple la pseudonymisation et l'anonymisation d'ensembles de données, ainsi que la fourniture de données dans des environnements de traitement sécurisés.

4. Dans l'accomplissement de leurs tâches, les organismes responsables de l'accès aux données de santé coopèrent activement avec les représentants des parties prenantes concernées, en particulier avec les représentants des patients, des détenteurs de données de santé et des utilisateurs de données de santé, et évitent tout conflit d'intérêts.

5. Dans l'accomplissement de leurs tâches et l'exercice de leurs pouvoirs, les organismes responsables de l'accès aux données de santé évitent tout conflit d'intérêts. Le personnel des organismes responsables de l'accès aux données de santé agit dans l'intérêt public et de manière indépendante.

6. Les États membres informent la Commission de l'identité des organismes responsables de l'accès aux données de santé désignés en vertu du paragraphe 1 au plus tard le 26 mars 2027. Ils informent également la Commission de toute modification ultérieure concernant l'identité de ces organismes. La Commission et les États membres mettent ces informations à la disposition du public.

Article 56

Service d'accès aux données de santé de l'Union

1. La Commission accomplit les tâches énoncées aux articles 57 et 59 lorsque les détenteurs de données de santé sont des institutions, organes et organismes de l'Union.

2. La Commission veille à ce que les ressources humaines, techniques et financières, les locaux et les infrastructures nécessaires soient alloués en vue de l'accomplissement efficace des tâches énoncées aux articles 57 et 59 et de l'exercice de ses fonctions.

3. Sauf exclusion explicite, les références aux organismes responsables de l'accès aux données de santé dans le présent règlement en ce qui concerne l'accomplissement des tâches et l'exercice des fonctions s'entendent comme s'appliquant également à la Commission lorsque les détenteurs de données de santé sont des institutions, organes et organismes de l'Union.

Article 57

Tâches des organismes responsables de l'accès aux données de santé

1. Les organismes responsables de l'accès aux données de santé accomplissent les tâches suivantes:

a) statuer sur les demandes d'accès aux données de santé en vertu de l'article 67 du présent règlement, autoriser et délivrer les autorisations de traitement de données en vertu de l'article 68 du présent règlement pour l'accès, à des fins d'utilisation secondaire, aux données de santé électroniques relevant de leur compétence, et statuer sur les demandes de données de santé présentées en vertu de l'article 69 du présent règlement conformément au présent chapitre et au chapitre II du règlement (UE) 2022/868, notamment pour ce qui est de:

   i) donner accès aux données de santé électroniques aux utilisateurs de données de santé en vertu d'une autorisation de traitement de données dans un environnement de traitement sécurisé, conformément à l'article 73;

   ii) surveiller et contrôler le respect des exigences énoncées dans le présent règlement par les utilisateurs de données de santé et les détenteurs de données de santé;

   iii) demander les données de santé électroniques visées à l'article 51 aux détenteurs de données de santé concernés en vertu d'une autorisation de traitement de données délivrée ou d'une demande de données de santé approuvée;

b) traiter les données de santé électroniques visées à l'article 51, notamment en assurant la réception, la combinaison, la préparation et la compilation de ces données lorsqu'elles sont demandées aux détenteurs de données de santé ainsi que la pseudonymisation ou l'anonymisation de ces données;

c) prendre toutes les mesures nécessaires pour préserver la confidentialité des droits de propriété intellectuelle, pour assurer la protection réglementaire des données et pour préserver la confidentialité des secrets d'affaires conformément à l'article 52, en tenant compte des droits pertinents dont disposent tant le détenteur de données de santé que l'utilisateur de données de santé;

d) coopérer avec les détenteurs de données de santé et les superviser afin de garantir la mise en œuvre cohérente et précise des dispositions sur le label de qualité et d'utilité des données prévues à l'article 78;

e) maintenir un système de gestion permettant d'enregistrer et de traiter les demandes d'accès aux données de santé, les demandes de données de santé, les décisions relatives à ces demandes, ainsi que les autorisations de traitement de données délivrées et les demandes de données de santé traitées, fournissant au moins des informations sur le nom du demandeur de données de santé, sur la finalité de l'accès, sur la date de délivrance et sur la durée de l'autorisation de traitement de données ainsi qu'une description de la demande d'accès aux données de santé ou de la demande de données de santé;

f) maintenir un système d'information du public afin de satisfaire aux obligations énoncées à l'article 58;

g) coopérer à l'échelon de l'Union et à l'échelon national afin d'établir des normes communes, des exigences techniques et des mesures appropriées pour l'accès aux données de santé électroniques dans un environnement de traitement sécurisé;

h) coopérer à l'échelon de l'Union et à l'échelon national et conseiller la Commission sur les techniques et les bonnes pratiques en matière d'utilisation secondaire et de gestion des données de santé électroniques;

i) faciliter l'accès transfrontière, à des fins d'utilisation secondaire, aux données de santé électroniques hébergées dans d'autres États membres par l'intermédiaire de DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75, et coopérer étroitement entre eux et avec la Commission.

j) rendre publics, par voie électronique:

   i) un catalogue des ensembles de données national, contenant des informations détaillées sur la source et la nature des données de santé électroniques, conformément aux articles 77, 78 et 80, et sur les conditions de mise à disposition de ces données;

   ii) toute demande d'accès aux données de santé et toute demande de données de santé sans retard indu après leur réception initiale;

   iii) toutes les autorisations de traitement de données délivrées ou toutes les demandes de données de santé approuvées ainsi que les décisions de refus, accompagnées d'une justification, dans les 30 jours ouvrables à compter de la délivrance, de l'approbation ou du refus;

   iv) les mesures liées au non-respect en vertu de l'article 63;

   v) les résultats communiqués par les utilisateurs de données de santé en vertu de l'article 61, paragraphe 4;

   vi) un système d'information afin de satisfaire aux obligations fixées à l'article 58;

   vii) des informations, au moins sur un site internet ou un portail internet facilement accessibles, sur la connexion à DonnéesDeSanté@UE (HealthData@EU) des points de contact nationaux à des fins d'utilisation secondaire d'un pays tiers ou d'un système établi au niveau international par une organisation internationale, dès que le pays tiers ou l'organisation internationale devient un participant autorisé à DonnéesDeSanté@UE (HealthData@EU);

k) s'acquitter des obligations envers les personnes physiques en vertu de l'article 58;

l) accomplir toute autre tâche visant à rendre possible une utilisation secondaire des données de santé électroniques dans le cadre du présent règlement.

Le catalogue des ensembles de données national visé au point j), i), du présent paragraphe est également mis à la disposition des points d'information uniques prévus à l'article 8 du règlement (UE) 2022/868.

2. Dans l'accomplissement de leurs tâches, les organismes responsables de l'accès aux données de santé:

a) coopèrent avec les autorités de contrôle au titre du règlement (UE) 2016/679 en ce qui concerne les données de santé électroniques à caractère personnel, ainsi qu'avec le comité de l'EEDS;

b) coopèrent avec toutes les parties prenantes concernées, dont les organisations de patients, les représentants de personnes physiques, les professionnels de la santé, les chercheurs et les comités d'éthique, le cas échéant conformément au droit de l'Union ou au droit national;

c) coopèrent avec d'autres organismes nationaux compétents, dont les autorités nationales compétentes chargées de la surveillance des organisations altruistes en matière de données au titre du règlement (UE) 2022/868, les autorités compétentes au titre du règlement (UE) 2023/2854 et les autorités nationales compétentes au titre des règlements (UE) 2017/745, (UE) 2017/746 et (UE) 2024/1689, le cas échéant.

3. Les organismes responsables de l'accès aux données de santé peuvent fournir une assistance aux organismes du secteur public lorsque ces derniers accèdent à des données de santé électroniques conformément à l'article 14 du règlement (UE) 2023/2854.

4. Les organismes responsables de l'accès aux données de santé peuvent soutenir un organisme du secteur public lorsqu'il obtient des données dans les situations visées à l'article 15, point a) ou b), du règlement (UE) 2023/2854, conformément aux règles fixées dans ledit règlement, en l'aidant sur le plan technique à traiter ces données ou à les combiner avec d'autres données en vue d'une analyse conjointe.

Article 58

Obligations des organismes responsables de l'accès aux données de santé à l'égard des personnes physiques

1. Les organismes responsables de l'accès aux données de santé mettent à la disposition du public les informations sur les conditions dans lesquelles les données de santé électroniques sont mises à disposition à des fins d'utilisation secondaire et rendent ces informations facilement consultables par voie électronique et accessibles pour les personnes physiques. Ces informations couvrent ce qui suit:

a) la base juridique en vertu de laquelle l'accès aux données de santé électroniques est octroyé à l'utilisateur de données de santé;

b) les mesures techniques et organisationnelles prises pour protéger les droits des personnes physiques;

c) les droits applicables des personnes physiques en matière d'utilisation secondaire;

d) les modalités selon lesquelles les personnes physiques peuvent exercer leurs droits conformément au chapitre III du règlement (UE) 2016/679;

e) l'identité et les coordonnées de l'organisme responsable de l'accès aux données de santé;

f) qui a été autorisé à accéder à des ensembles de données de santé électroniques et à quels ensembles de données l'accès leur a été octroyé ainsi que les détails de l'autorisation de traitement de données en ce qui concerne les finalités du traitement de ces données, conformément à l'article 53, paragraphe 1;

g) les résultats ou l'aboutissement des projets pour lesquels les données de santé électroniques ont été utilisées.

2. Si un État membre prévoit un droit de refus en vertu de l'article 71 devant être exercé par l'intermédiaire des organismes responsables de l'accès aux données de santé, les organismes responsables de l'accès aux données de santé concernés fournissent au public des informations sur la procédure relative au droit de refus et facilitent l'exercice de ce droit.

3. Lorsqu'un organisme responsable de l'accès aux données de santé est informé par un utilisateur de données de santé d'une constatation significative relative à la santé d'une personne physique, conformément à l'article 61, paragraphe 5, il informe le détenteur de données de santé de cette constatation. Le détenteur de données de santé informe, dans les conditions prévues par le droit national, la personne physique ou le professionnel de la santé traitant la personne physique concernée. Les personnes physiques ont le droit de demander à ne pas être informées de ces constatations.

4. Les États membres informent le grand public sur le rôle et les avantages des organismes responsables de l'accès aux données de santé.

Article 59

Rapports des organismes responsables de l'accès aux données de santé

1. Chaque organisme responsable de l'accès aux données de santé publie un rapport d'activité tous les deux ans et le met à la disposition du public sur son site internet. Si un État membre désigne plusieurs organismes responsables de l'accès aux données de santé, l'organisme de coordination visé à l'article 55, paragraphe 1, est responsable du rapport d'activité et demande les informations nécessaires aux autres organismes responsables de l'accès aux données de santé. Ce rapport d'activité suit une structure convenue par le comité de l'EEDS en vertu de l'article 94, paragraphe 2, point d), et contient au moins les catégories d'informations suivantes:

a) des informations sur les demandes d'accès aux données de santé et sur les demandes de données de santé présentées, telles que les types de demandeurs de données de santé, le nombre d'autorisations de traitement de données délivrées ou refusées, les catégories de finalités d'accès et les catégories de données de santé électroniques auxquelles il a été accédé, ainsi qu'un résumé des résultats des utilisations de données de santé électroniques, le cas échéant;

b) des informations sur le respect des engagements réglementaires et contractuels par les utilisateurs de données de santé et les détenteurs de données de santé, ainsi que le nombre d'amendes administratives imposées par les organismes responsables de l'accès aux données de santé et leur montant;

c) des informations sur les audits réalisés concernant les utilisateurs de données de santé pour veiller à la conformité du traitement qu'ils ont effectué dans l'environnement de traitement sécurisé en vertu de l'article 73, paragraphe 1, point e);

d) des informations sur les audits internes et de tiers relatifs à la conformité des environnements de traitement sécurisés avec les normes, spécifications et exigences définies, conformément à l'article 73, paragraphe 3;

e) des informations sur le traitement des demandes des personnes physiques concernant l'exercice de leurs droits à la protection des données;

f) une description des activités de l'organisme responsable de l'accès aux données de santé réalisées en ce qui concerne le dialogue avec les parties prenantes concernées et la consultation desdites parties prenantes concernées;

g) les recettes provenant des autorisations de traitement de données et des demandes de données de santé;

h) le nombre moyen de jours entre les demandes d'accès aux données de santé ou les demandes de données de santé et l'accès aux données;

i) le nombre de labels de qualité des données délivrés par les détenteurs de données de santé, ventilé par catégorie de qualité;

j) le nombre de publications de recherche évaluées par des pairs, de documents d'orientation et de procédures réglementaires utilisant des données auxquelles il a été accédé via l'EEDS;

k) le nombre de produits et services de santé numériques, dont les applications d'IA, mis au point grâce à des données auxquelles il a été accédé via l'EEDS.

2. Le rapport d'activité visé au paragraphe 1 est présenté à la Commission et au comité de l'EEDS dans un délai de six mois à compter de la fin de la deuxième année de la période sur laquelle porte le rapport concerné. Le rapport d'activité est accessible via le site internet de la Commission.

Article 60

Obligations des détenteurs de données de santé

1. Les détenteurs de données de santé mettent les données de santé électroniques pertinentes visées à l'article 51, sur demande, à la disposition de l'organisme responsable de l'accès aux données de santé conformément à une autorisation de traitement de données délivrée en vertu de l'article 68 ou à une demande de données de santé approuvée en vertu de l'article 69.

2. Les détenteurs des données de santé mettent les données de santé électroniques demandées visées au paragraphe 1 à la disposition de l'organisme responsable de l'accès aux données de santé dans un délai raisonnable et au plus tard trois mois à compter de la réception de la demande de l'organisme responsable de l'accès aux données de santé. Dans des cas justifiés, l'organisme responsable de l'accès aux données de santé peut prolonger ce délai de trois mois au maximum.

3. Le détenteur de données de santé communique à l'organisme responsable de l'accès aux données de santé une description de l'ensemble de données qu'il détient conformément à l'article 77. Le détenteur de données de santé vérifie, au minimum une fois par an, que sa description de l'ensemble de données figurant dans le catalogue des ensembles de données national est exacte et à jour.

4. Lorsqu'un label de qualité et d'utilité des données accompagne l'ensemble de données en vertu de l'article 78, le détenteur de données de santé fournit à l'organisme responsable de l'accès aux données de santé des documents suffisants pour lui permettre de vérifier l'exactitude du label.

5. Les détenteurs de données de santé électroniques à caractère non personnel donnent accès aux données au moyen de bases de données ouvertes et fiables afin de garantir un accès illimité à tous les utilisateurs ainsi que le stockage et la conservation des données. Les bases de données publiques ouvertes et fiables disposent d'une gouvernance solide, transparente et durable et d'un modèle transparent d'accès des utilisateurs.

Article 61

Obligations des utilisateurs de données de santé

1. Les utilisateurs de données de santé peuvent accéder aux données de santé électroniques visées à l'article 51 à des fins d'utilisation secondaire et les traiter uniquement conformément à une autorisation de traitement de données délivrée en vertu de l'article 68, une demande de données de santé approuvée en vertu de l'article 69 ou, dans les situations visées à l'article 67, paragraphe 3, une approbation d'accès émanant du participant autorisé à DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75 concerné.

2. Lorsqu'ils traitent des données de santé électroniques dans les environnements de traitement sécurisés visés à l'article 73, les utilisateurs de données de santé ne peuvent pas donner accès aux données de santé électroniques à des tiers qui ne figurent pas dans l'autorisation de traitement de données, ou mettre ces données à la disposition de tels tiers.

3. Les utilisateurs de données de santé ne peuvent pas réidentifier ou tenter de réidentifier les personnes physiques auxquelles se rapportent les données de santé électroniques qu'ils ont obtenues sur la base d'une autorisation de traitement de données, d'une demande de données de santé ou d'une approbation d'accès émanant d'un participant autorisé à DonnéesDeSanté@UE (HealthData@EU).

4. Les utilisateurs de données de santé rendent publics les résultats ou l'aboutissement de l'utilisation secondaire, y compris les informations pertinentes pour la prestation de soins de santé, dans un délai de 18 mois à compter de l'achèvement du traitement des données de santé électroniques dans l'environnement de traitement sécurisé ou à compter de la réception de la réponse à la demande de données de santé visée à l'article 69.

Dans des cas justifiés liés aux finalités autorisées du traitement des données de santé électroniques, le délai visé au premier alinéa peut être prolongé par l'organisme responsable de l'accès aux données de santé, en particulier dans les cas où le résultat est publié dans une revue scientifique ou une autre publication scientifique.

Les résultats ou l'aboutissement de l'utilisation secondaire ne contiennent que des données anonymisées.

Les utilisateurs de données de santé informent les organismes responsables de l'accès aux données de santé auprès desquels une autorisation de traitement de données a été obtenue des résultats ou de l'aboutissement de l'utilisation secondaire et les aident à rendre ces informations publiques sur les sites internet des organismes responsables de l'accès aux données de santé. Cette publication est sans préjudice des droits de publication dans des revues scientifiques ou d'autres publications scientifiques.

Lorsque les utilisateurs de données de santé utilisent des données de santé électroniques conformément au présent chapitre, ils reconnaissent les sources des données de santé électroniques et le fait que les données de santé électroniques ont été obtenues dans le cadre de l'EEDS.

5. Sans préjudice du paragraphe 2, les utilisateurs de données de santé informent l'organisme responsable de l'accès aux données de santé de toute constatation significative relative à l'état de santé de la personne physique dont les données sont incluses dans l'ensemble de données.

6. Les utilisateurs de données de santé coopèrent avec les organismes responsables de l'accès aux données de santé dans l'accomplissement des tâches desdits organismes.

Article 62

Redevances

1. Les organismes responsables de l'accès aux données de santé, y compris le service d'accès aux données de santé de l'Union, ou les détenteurs de données de santé de confiance visés à l'article 72 peuvent percevoir des redevances pour la mise à disposition de données de santé électroniques à des fins d'utilisation secondaire.

Les redevances sont proportionnelles au coût de la mise à disposition des données et ne restreignent pas la concurrence.

Les redevances couvrent tout ou partie des coûts liés à la procédure d'évaluation d'une demande d'accès aux données de santé ou d'une demande de données de santé, de délivrance, de refus ou de modification d'une autorisation de traitement de données en vertu des articles 67 et 68, ou de réponse à une demande de données de santé présentée en vertu de l'article 69, y compris les coûts liés à la consolidation, à la préparation, à la pseudonymisation, à l'anonymisation et à la fourniture de données de santé électroniques.

Les États membres peuvent fixer des redevances réduites pour certains types d'utilisateurs de données de santé situés dans l'Union, tels que les organismes du secteur public ou les institutions, organes et organismes de l'Union ayant un mandat légal dans le domaine de la santé publique, les chercheurs universitaires ou les microentreprises.

2. Les redevances visées au paragraphe 1 du présent article peuvent inclure une compensation pour les coûts exposés par le détenteur de données de santé pour la compilation et la préparation des données de santé électroniques à mettre à disposition à des fins d'utilisation secondaire. En pareils cas, le détenteur de données de santé fournit une estimation de ces coûts à l'organisme responsable de l'accès aux données de santé. Lorsque le détenteur de données de santé est un organisme du secteur public, l'article 6 du règlement (UE) 2022/868 ne s'applique pas. La partie des redevances liée aux coûts du détenteur de données de santé est versée au détenteur de données de santé.

3. Toutes redevances facturées aux utilisateurs de données de santé en vertu du présent article sont transparentes et non discriminatoires.

4. Lorsque les détenteurs de données de santé et les utilisateurs de données de santé ne s'accordent pas sur le montant des redevances dans un délai d'un mois à compter de la délivrance de l'autorisation de traitement de données, l'organisme responsable de l'accès aux données de santé peut fixer les redevances en proportion du coût de la mise à disposition de données de santé électroniques à des fins d'utilisation secondaire. Lorsque les détenteurs de données de santé ou les utilisateurs de données de santé se trouvent en désaccord sur la redevance fixée par l'organisme responsable de l'accès aux données de santé, ils ont accès aux organes de règlement des litiges conformément à l'article 10 du règlement (UE) 2023/2854.

5. Avant de délivrer une autorisation de traitement de données en vertu de l'article 68 ou de répondre à une demande de données de santé présentée en vertu de l'article 69, l'organisme responsable de l'accès aux données de santé informe le demandeur de données de santé des redevances estimées. Le demandeur de données de santé est informé de la possibilité de retirer sa demande d'accès aux données de santé ou sa demande de données de santé. Si le demandeur de données de santé retire sa demande, seuls les coûts déjà exposés lui sont facturés.

6. La Commission établit, par voie d'actes d'exécution, des principes applicables aux politiques et aux structures liées aux redevances, y compris aux déductions en faveur des entités visées au paragraphe 1, quatrième alinéa, du présent article de manière à favoriser la cohérence et la transparence entre les États membres en ce qui concerne ces politiques et ces structures liées aux redevances. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 63

Exécution par les organismes responsables de l'accès aux données de santé

1. Lorsqu'ils accomplissent leurs tâches de surveillance et de contrôle visées à l'article 57, paragraphe 1, point a), ii), les organismes responsables de l'accès aux données de santé ont le droit de demander et d'obtenir toutes les informations nécessaires des utilisateurs de données de santé et des détenteurs de données de santé pour vérifier la conformité avec le présent chapitre.

2. Lorsque les organismes responsables de l'accès aux données de santé constatent qu'un utilisateur de données de santé ou un détenteur de données de santé ne se conforme pas aux exigences du présent chapitre, ils notifient immédiatement ces constatations à l'utilisateur de données de santé ou au détenteur de données de santé et prennent des mesures appropriées. L'organisme responsable de l'accès aux données de santé concerné donne à l'utilisateur de données de santé ou au détenteur de données de santé concerné la possibilité d'exprimer son point de vue dans un délai raisonnable qui ne dépasse pas quatre semaines.

Lorsque la constatation de non-conformité concerne une éventuelle violation du règlement (UE) 2016/679, l'organisme responsable de l'accès aux données de santé concerné en informe immédiatement les autorités de contrôle au titre dudit règlement et leur fournit toutes les informations pertinentes au sujet de cette constatation.

3. En cas de non-conformité de la part d'utilisateurs de données de santé, les organismes responsables de l'accès aux données de santé ont le pouvoir de révoquer l'autorisation de traitement de données délivrée en vertu de l'article 68 et d'arrêter, sans retard indu, l'opération de traitement de données de santé électroniques concernée effectuée par l'utilisateur de données de santé, et ils prennent des mesures appropriées et proportionnées pour veiller à ce que le traitement par l'utilisateur de données de santé soit conforme.

En outre, dans le cadre de telles mesures d'exécution, les organismes responsables de l'accès aux données de santé peuvent, le cas échéant, exclure ou engager une procédure en vue d'exclure, conformément au droit national, l'utilisateur de données de santé concerné de tout accès aux données de santé électroniques au sein de l'EEDS dans le contexte d'une utilisation secondaire pendant une période maximale de cinq ans.

4. En cas de non-conformité de la part de détenteurs de données de santé, lorsqu'un détenteur de données de santé retient les données de santé électroniques des organismes responsables de l'accès aux données de santé dans l'intention manifeste d'en entraver l'utilisation, ou ne respecte pas les délais fixés à l'article 60, paragraphe 2, l'organisme responsable de l'accès aux données de santé a le pouvoir d'infliger au détenteur de données de santé une astreinte, transparente et proportionnée, pour chaque jour de retard. Le montant des amendes est fixé par l'organisme responsable de l'accès aux données de santé conformément au droit national. En cas de manquements répétés du détenteur de données de santé à l'obligation de coopération avec l'organisme responsable de l'accès aux données de santé, ledit organisme peut exclure ou engager une procédure en vue d'exclure, conformément au droit national, le détenteur de données de santé concerné de la possibilité de présenter des demandes d'accès aux données de santé en vertu du présent chapitre pendant une période maximale de cinq ans. Pendant cette période d'exclusion, le détenteur de données de santé reste tenu de rendre les données accessibles au titre du présent chapitre, le cas échéant.

5. L'organisme responsable de l'accès aux données de santé communique, sans retard, à l'utilisateur de données de santé ou au détenteur de données de santé concerné les mesures d'exécution prises en vertu des paragraphes 3 et 4 et les motifs sur lesquels elles se fondent, et il fixe un délai raisonnable pour que l'utilisateur de données de santé ou le détenteur de données de santé se conforme auxdites mesures.

6. Toutes mesures d'exécution prises par l'organisme responsable de l'accès aux données de santé en vertu du paragraphe 3 sont notifiées aux autres organismes responsables de l'accès aux données de santé, au moyen de l'outil informatique visé au paragraphe 7. Les organismes responsables de l'accès aux données de santé peuvent mettre ces informations à la disposition du public sur leurs sites internet.

7. La Commission détermine, par voie d'actes d'exécution, l'architecture d'un outil informatique, dans le cadre de l'infrastructure DonnéesDeSanté@UE (HealthData@EU) visée à l'article 75, destiné à soutenir les mesures d'exécution visées au présent article, en particulier les astreintes, les révocations d'autorisations de traitement de données et les exclusions, et à rendre ces mesures d'exécution transparentes pour d'autres organismes responsables de l'accès aux données de santé. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

8. La Commission publie, au plus tard le 26 mars 2032, en étroite coopération avec le comité de l'EEDS, des lignes directrices sur les mesures d'exécution, y compris les astreintes et autres mesures à prendre par les organismes responsables de l'accès aux données de santé.

Article 64

Conditions générales d'imposition d'amendes administratives par les organismes responsables de l'accès aux données de santé

1. Chaque organisme responsable de l'accès aux données de santé veille à ce que les amendes administratives imposées en vertu du présent article pour des violations visées aux paragraphes 4 et 5 soient, dans chaque cas individuel, effectives, proportionnées et dissuasives.

2. Selon les circonstances propres à chaque cas individuel, les amendes administratives sont imposées en complément ou à la place des mesures d'exécution visées à l'article 63, paragraphes 3 et 4. Les organismes responsables de l'accès aux données de santé décident s'il convient d'imposer une amende administrative et du montant de l'amende administrative dans chaque cas individuel, en tenant dûment compte des éléments suivants:

a) la nature, la gravité et la durée de la violation;

b) la question de savoir si des sanctions ou des amendes administratives ont déjà été imposées par d'autres autorités compétentes pour la même violation;

c) le fait que la violation a été commise délibérément ou par négligence;

d) toute mesure prise par le détenteur de données de santé ou l'utilisateur de données de santé pour atténuer le dommage causé;

e) le degré de responsabilité de l'utilisateur de données de santé, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre en vertu de l'article 67, paragraphe 2, point g), et de l'article 67, paragraphe 4;

f) toute violation antérieure pertinente commise par le détenteur de données de santé ou l'utilisateur de données de santé;

g) le degré de coopération établi par le détenteur de données de santé ou l'utilisateur de données de santé avec l'organisme responsable de l'accès aux données de santé en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

h) la manière dont l'organisme responsable de l'accès aux données de santé a eu connaissance de la violation, notamment si, et dans quelle mesure, l'utilisateur des données de santé lui a notifié la violation;

i) le respect de toutes mesures d'exécution visées à l'article 63, paragraphes 3 et 4, qui ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet;

j) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

3. Si le détenteur de données de santé ou l'utilisateur de données de santé viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même autorisation de traitement de données ou demande de données de santé ou d'autorisations ou de demandes liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4. Conformément au paragraphe 2 du présent article, les violations des obligations du détenteur de données de santé ou de l'utilisateur de données de santé en vertu de l'article 60 et de l'article 61, paragraphes 1, 5 et 6, font l'objet d'amendes administratives pouvant s'élever à maximum 10 000 000 EUR ou, dans le cas d'une entreprise, à maximum 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

5. Conformément au paragraphe 2, les violations suivantes font l'objet, d'amendes administratives pouvant s'élever à maximum 20 000 000 EUR ou, dans le cas d'une entreprise, à maximum 4 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

a) le traitement, par des utilisateurs de données de santé, de données de santé électroniques obtenues au moyen d'une autorisation de traitement de données délivrée en vertu de l'article 68 aux fins des utilisations visées à l'article 54;

b) l'extraction, par les utilisateurs de données de santé, de données de santé électroniques à caractère personnel à partir d'environnements de traitement sécurisés;

c) la réidentification ou la tentative de réidentification des personnes physiques auxquelles se rapportent les données de santé électroniques obtenues par les utilisateurs de données de santé sur la base d'une autorisation de traitement de données ou d'une demande de données de santé en vertu de l'article 61, paragraphe 3;

d) le non-respect des mesures d'exécution prises par l'organisme responsable de l'accès aux données de santé en vertu de l'article 63, paragraphes 3 et 4.

6. Sans préjudice des pouvoirs dont les organismes responsables de l'accès aux données de santé disposent en vertu de l'article 63, chaque État membre peut établir des règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes du secteur public établis sur le territoire dudit État membre.

7. L'exercice, par un organisme responsable de l'accès aux données de santé, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit national, y compris des recours juridictionnels effectifs et une procédure régulière.

8. Lorsque le système juridique d'un État membre ne prévoit pas d'amendes administratives, il est possible d'appliquer le présent article de sorte que, conformément à son cadre juridique national, ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les organismes responsables de l'accès aux données de santé. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. L'État membre concerné notifie à la Commission les dispositions de droit qu'il adopte en vertu du présent paragraphe au plus tard le 26 mars 2029 et, sans retard, toute législation ultérieure modifiant ces dispositions ou toutes modifications concernant ces dispositions.

Article 65

Relations avec les autorités de contrôle en vertu du règlement (UE) 2016/679

L'autorité de contrôle ou les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 et de veiller au respect de celui-ci sont également compétentes pour surveiller l'application du droit de refuser le traitement des données de santé électroniques à caractère personnel à des fins d'utilisation secondaire en vertu de l'article 71 ainsi que pour veiller au respect de ce droit. Ces autorités de contrôle sont habilitées à imposer des amendes administratives à concurrence du montant visé à l'article 83 du règlement (UE) 2016/679.

Le cas échéant, les autorités de contrôle visées au premier alinéa du présent article et les organismes responsables de l'accès aux données de santé visés à l'article 55 du présent règlement coopèrent aux fins de l'exécution du présent règlement, dans les limites de leurs compétences respectives. Les dispositions pertinentes du règlement (UE) 2016/679 s'appliquent mutatis mutandis.

SECTION 3

Accès aux données de santé électroniques à des fins d'utilisation secondaire

Article 66

Minimisation des données et limitation des finalités

1. Lorsque les organismes responsables de l'accès aux données de santé reçoivent une demande d'accès aux données de santé, ils veillent à ce que l'accès soit donné uniquement aux données de santé électroniques qui sont appropriées, pertinentes et limitées à ce qui est nécessaire au regard de la finalité du traitement dont il est fait mention dans la demande d'accès aux données de santé présentée par l'utilisateur de données de santé, et dans le respect de l'autorisation de traitement de données qui a été délivrée en vertu de l'article 68.

2. Les organismes responsables de l'accès aux données de santé fournissent les données de santé électroniques dans un format anonymisé, lorsque la finalité du traitement par l'utilisateur de données de santé peut être réalisée à l'aide de ces données, compte tenu des informations fournies par l'utilisateur de données de santé.

3. Lorsque l'utilisateur de données de santé a suffisamment démontré que la finalité du traitement ne peut pas être réalisée à l'aide de données anonymisées conformément à l'article 68, paragraphe 1, point c), les organismes responsables de l'accès aux données de santé donnent accès aux données de santé électroniques dans un format pseudonymisé. Les informations nécessaires pour annuler la pseudonymisation ne sont accessibles qu'à l'organisme responsable de l'accès aux données de santé ou à une entité qui agit en tant que tiers de confiance conformément au droit national.

Article 67

Demandes d'accès aux données de santé

1. Une personne physique ou morale peut présenter à un organisme responsable de l'accès aux données de santé une demande d'accès aux données de santé pour les finalités visées à l'article 53, paragraphe 1.

2. La demande d'accès aux données de santé comprend:

a) l'identité du demandeur de données de santé, une description de ses fonctions et de ses activités professionnelles, y compris l'identité des personnes physiques qui auraient accès aux données de santé électroniques si une autorisation de traitement de données était délivrée; le demandeur de données de santé notifie à l'organisme responsable de l'accès aux données de santé toute mise à jour de la liste des personnes physiques;

b) les finalités visées à l'article 53, paragraphe 1, pour lesquelles l'accès est demandé;

c) une explication détaillée de l'utilisation prévue des données de santé électroniques et des avantages escomptés liés à cette utilisation, ainsi que de la manière dont ces avantages contribueraient aux finalités visées à l'article 53, paragraphe 1;

d) une description des données de santé électroniques demandées, notamment leur portée, la période concernée, leur format, leurs sources et, si possible, la couverture géographique lorsque ces données sont demandées à des détenteurs de données de santé de plusieurs États membres ou à des participants autorisés à DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75;

e) une description indiquant si les données de santé électroniques doivent être mises à disposition dans un format pseudonymisé ou anonymisé; dans le cas d'un format pseudonymisé, une justification de la raison pour laquelle le traitement ne peut être effectué à l'aide de données anonymisées;

f) lorsque le demandeur de données de santé a l'intention d'introduire des ensembles de données qu'il détient déjà dans l'environnement de traitement sécurisé, une description de ces ensembles de données;

g) une description des garanties, qui doivent être proportionnées aux risques, prévues pour empêcher toute utilisation abusive des données de santé électroniques, ainsi que pour protéger les droits et intérêts du détenteur de données de santé et des personnes physiques concernées, et notamment pour empêcher toute réidentification des personnes physiques dans l'ensemble de données;

h) une indication justifiée de la période pendant laquelle les données de santé électroniques sont nécessaires au traitement dans un environnement de traitement sécurisé;

i) une description des outils et des ressources informatiques nécessaires à un environnement de traitement sécurisé;

j) le cas échéant, des informations sur toute évaluation des aspects éthiques du traitement, requise au titre du droit national, qui peut servir à remplacer la propre évaluation éthique du demandeur de données de santé;

k) lorsque le demandeur de données de santé a l'intention de faire usage d'une exception au titre de l'article 71, paragraphe 4, la justification requise par le droit national en vertu dudit article.

3. Lorsque le demandeur de données de santé cherche à accéder à des données de santé électroniques détenues par des détenteurs de données de santé établis dans plus d'un État membre ou des participants autorisés à DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75 concernés, il soumet une demande unique d'accès aux données de santé par l'intermédiaire de l'organisme responsable de l'accès aux données de santé de l'État membre dans lequel l'établissement principal du demandeur de données de santé est situé, par l'intermédiaire de l'organisme responsable de l'accès aux données de santé de l'État membre dans lequel l'un de ces détenteurs de données de santé est établi ou par l'intermédiaire des services fournis par la Commission dans DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75. La demande d'accès aux données de santé est automatiquement transmise aux participants autorisés à DonnéesDeSanté@UE (HealthData@EU) concernés et aux organismes responsables de l'accès aux données de santé des États membres dans lesquels sont établis les détenteurs de données de santé identifiés dans la demande d'accès aux données de santé.

4. Lorsque le demandeur de données de santé cherche à accéder aux données de santé électroniques à caractère personnel dans un format pseudonymisé, il fournit, avec la demande d'accès aux données de santé, une description de la manière dont le traitement serait conforme au droit de l'Union et au droit national applicables en matière de protection des données et de respect de la vie privée, notamment au règlement (UE) 2016/679 et, en particulier, à l'article 6, paragraphe 1, dudit règlement.

5. Les organismes du secteur public et les institutions, organes et organismes de l'Union fournissent les mêmes informations que celles requises en vertu des paragraphes 2 et 4, à l'exception du paragraphe 2, point h), auquel cas ils communiquent, à la place, des informations sur la période pendant laquelle il est possible d'accéder aux données de santé électroniques, sur la fréquence de cet accès ou sur la fréquence des mises à jour des données.

Article 68

Autorisation de traitement de données

1. Aux fins de donner accès aux données de santé électroniques, les organismes responsables de l'accès aux données de santé évaluent si tous les critères suivants sont remplis:

a) les finalités décrites dans la demande d'accès aux données de santé correspondent à une ou plusieurs des finalités énumérées à l'article 53, paragraphe 1;

b) les données demandées sont nécessaires, adéquates et proportionnées aux finalités décrites dans la demande d'accès aux données de santé, compte tenu des exigences de minimisation des données et de limitation des finalités prévues à l'article 66;

c) le traitement est conforme à l'article 6, paragraphe 1, du règlement (UE) 2016/679, et, dans le cas de données pseudonymisées, il existe une justification suffisante de ce que la finalité ne peut pas être réalisée à l'aide de données anonymisées;

d) le demandeur de données de santé est qualifié au regard des finalités prévues de l'utilisation des données et possède une expertise appropriée, notamment des qualifications professionnelles dans les domaines des soins de santé, des soins, de la santé publique ou de la recherche, et cohérente avec les pratiques éthiques et les lois et réglementations applicables;

e) le demandeur de données de santé démontre l'existence de mesures techniques et organisationnelles suffisantes pour prévenir une utilisation abusive des données de santé électroniques et protéger les droits et les intérêts du détenteur de données de santé et des personnes physiques concernées;

f) les informations sur l'évaluation des aspects éthiques du traitement, visée à l'article 67, paragraphe 2, point j), le cas échéant, respectent le droit national;

g) lorsque le demandeur de données de santé a l'intention de faire usage d'une exception au titre de l'article 71, paragraphe 4, la justification requise par les dispositions de droit national adoptées en vertu dudit article a été fournie;

h) le demandeur de données de santé remplit toutes les autres exigences prévues au présent chapitre.

2. L'organisme responsable de l'accès aux données de santé tient également compte de ce qui suit:

a) les risques pour la défense nationale, la sécurité, la sécurité publique et l'ordre public;

b) le risque de compromettre la confidentialité des données dans les bases de données gouvernementales des autorités réglementaires.

3. Lorsque l'organisme responsable de l'accès aux données de santé conclut que les exigences prévues au paragraphe 1 sont remplies et que les risques visés au paragraphe 2 sont suffisamment atténués, l'organisme responsable de l'accès aux données de santé octroie l'accès aux données de santé électroniques en délivrant une autorisation de traitement de données. Les organismes responsables de l'accès aux données de santé refusent toutes les demandes d'accès aux données de santé lorsque les exigences prévues au présent chapitre ne sont pas remplies.

Lorsque les exigences pour la délivrance d'une autorisation de traitement de données ne sont pas remplies, mais que les exigences pour fournir une réponse dans un format statistique anonymisé en vertu de l'article 69 le sont, l'organisme responsable de l'accès aux données de santé peut décider de fournir une telle réponse à condition que cette réponse atténue les risques et si la finalité de la demande d'accès aux données de santé peut être réalisée de cette manière, et que le demandeur de données de santé accepte de recevoir une réponse dans un format statistique anonymisé en vertu de l'article 69.

4. Par dérogation au règlement (UE) 2022/868, l'organisme responsable de l'accès aux données de santé délivre ou refuse de délivrer une autorisation de traitement de données dans un délai de trois mois à compter de la réception d'une demande complète d'accès aux données de santé. Si l'organisme responsable de l'accès aux données de santé constate que la demande d'accès aux données de santé est incomplète, il en informe le demandeur de données de santé et lui donne la possibilité de compléter cette demande. Si le demandeur de données de santé ne complète pas la demande d'accès aux données de santé dans un délai de quatre semaines, l'autorisation de traitement de données n'est pas délivrée.

L'organisme responsable de l'accès aux données de santé peut, si nécessaire, prolonger de trois mois supplémentaires le délai de réponse à une demande d'accès aux données de santé, compte tenu de l'urgence et de la complexité de la demande d'accès aux données de santé ainsi que du volume des demandes d'accès aux donnés de santé présentées en vue d'une décision. En pareils cas, l'organisme responsable de l'accès aux données de santé informe dès que possible le demandeur de données de santé qu'un délai supplémentaire est nécessaire pour l'examen de la demande d'accès aux donnés de santé, et lui communique en même temps les raisons du retard.

5. Lorsqu'ils traitent une demande d'accès aux données de santé pour un accès transfrontière à des données de santé électroniques visées à l'article 67, paragraphe 3, les organismes responsables de l'accès aux données de santé et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) visé à l'article 75 concernés conservent la responsabilité en ce qui concerne l'adoption des décisions d'octroyer ou de refuser l'accès aux données de santé électroniques relevant de leur compétence, conformément au présent chapitre.

Les organismes responsables de l'accès aux données de santé et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) concernés s'informent mutuellement de leurs décisions. Ils peuvent prendre ces informations en considération lorsqu'ils décident d'octroyer ou de refuser l'accès aux données de santé électroniques.

Une autorisation de traitement de données délivrée par un organisme responsable de l'accès aux données de santé peut bénéficier de la reconnaissance mutuelle des autres organismes responsables de l'accès aux données de santé.

6. Les États membres prévoient une procédure de demande d'accès aux données de santé accélérée pour les organismes du secteur public et les institutions, organes et organismes de l'Union dotés d'un mandat légal dans le domaine de la santé publique si le traitement des données de santé électroniques doit être effectué pour les finalités établies à l'article 53, paragraphe 1, points a), b) et c).

Lorsque cette procédure accélérée s'applique, l'organisme responsable de l'accès aux données de santé délivre ou refuse de délivrer une autorisation de traitement de données dans un délai de deux mois à compter de la réception d'une demande complète d'accès aux données de santé. L'organisme responsable de l'accès aux données de santé peut au besoin prolonger d'un mois supplémentaire le délai de réponse à une demande d'accès aux données de santé.

7. Après la délivrance de l'autorisation de traitement de données, l'organisme responsable de l'accès aux données de santé demande immédiatement les données de santé électroniques au détenteur de données de santé. L'organisme responsable de l'accès aux données de santé met les données de santé électroniques à la disposition de l'utilisateur de données de santé dans un délai de deux mois à compter du moment où il reçoit ces données des détenteurs de données de santé, sauf si l'organisme responsable de l'accès aux données de santé fait savoir qu'il fournira les données dans un délai plus long qu'il indique.

8. Dans les cas visés au paragraphe 5, premier alinéa, du présent article, les organismes responsables de l'accès aux données de santé et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) qui ont délivré une autorisation de traitement de données ou une approbation d'accès, respectivement, peuvent décider de donner accès aux données de santé électroniques dans l'environnement de traitement sécurisé fourni par la Commission conformément à l'article 75, paragraphe 9.

9. Lorsque l'organisme responsable de l'accès aux données de santé refuse de délivrer une autorisation de traitement de données, il fournit une justification de ce refus au demandeur de données de santé.

10. Lorsque l'organisme responsable de l'accès aux données de santé délivre une autorisation de traitement de données, il fixe dans cette autorisation de traitement de données les conditions générales applicables à l'utilisateur de données de santé. L'autorisation de traitement de données contient ce qui suit:

a) les catégories, la spécification et le format des données de santé électroniques auxquelles il doit être accédé, qui sont couvertes par l'autorisation de traitement de données, ainsi que les sources desdites données, et une indication quant à savoir si l'accès aux données de santé électroniques doit avoir lieu dans un format pseudonymisé dans l'environnement de traitement sécurisé;

b) une description détaillée de la finalité pour laquelle les données de santé électroniques sont mises à disposition;

c) lorsqu'un mécanisme pour mettre en œuvre une exception est prévu et s'applique au titre de l'article 71, paragraphe 4, des informations indiquant s'il a été appliqué et le motif de la décision qui y est liée;

d) l'identité des personnes autorisées, en particulier l'identité de l'investigateur principal, disposant de droits d'accès aux données de santé électroniques dans l'environnement de traitement sécurisé;

e) la durée de l'autorisation de traitement de données;

f) des informations sur les caractéristiques techniques et sur les outils dont dispose l'utilisateur de données de santé dans l'environnement de traitement sécurisé;

g) les redevances à payer par l'utilisateur de données de santé;

h) toutes conditions spécifiques.

11. Les utilisateurs de données de santé ont le droit d'accéder aux données de santé électroniques et de les traiter dans un environnement de traitement sécurisé conformément à l'autorisation de traitement de données qui leur a été délivrée sur la base du présent règlement.

12. Une autorisation de traitement de données est délivrée pour la durée nécessaire à la réalisation des finalités demandées et cette durée ne peut pas dépasser dix ans. Cette durée peut être prolongée une fois, pour une durée ne dépassant pas dix ans, à la demande de l'utilisateur de données de santé, sur la base d'arguments et de documents justifiant cette prolongation fournis un mois avant l'expiration de l'autorisation de traitement de données. L'organisme responsable de l'accès aux données de santé peut percevoir des redevances qui augmentent pour tenir compte des coûts et des risques associés au stockage des données de santé électroniques pendant une période dépassant la période initiale. Afin de réduire ces coûts et ces redevances, l'organisme responsable de l'accès aux données de santé peut également proposer à l'utilisateur de données de santé de stocker l'ensemble de données dans un système de stockage ayant des capacités réduites. Ces capacités réduites ne portent pas atteinte à la sécurité de l'ensemble de données traité. Les données de santé électroniques dans l'environnement de traitement sécurisé sont effacées dans un délai de six mois à compter de l'expiration de l'autorisation de traitement de données. À la demande de l'utilisateur de données de santé, la formule applicable à la création de l'ensemble de données demandé peut être conservée par l'organisme responsable de l'accès aux données de santé.

13. L'utilisateur de données de santé soumet une demande de modification de l'autorisation de traitement de données si celle-ci doit être mise à jour.

14. La Commission peut, par voie d'un acte d'exécution, établir un logo permettant de reconnaître la contribution de l'EEDS. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 69

Demande de données de santé

1. Le demandeur de données de santé peut présenter une demande de données de santé pour les finalités visées à l'article 53 dans le but d'obtenir une réponse uniquement dans un format statistique anonymisé. Un organisme responsable de l'accès aux données de santé ne fournit pas de réponse à une demande de données de santé dans un autre format, et l'utilisateur de données de santé n'a pas accès aux données de santé électroniques utilisées pour fournir cette réponse.

2. Une demande de données de santé visée au paragraphe 1 comprend les informations suivantes:

a) l'identité du demandeur de données de santé et une description de ses fonctions et de ses activités professionnelles;

b) une explication détaillée de l'utilisation prévue des données de santé électroniques, notamment les finalités visées à l'article 53, paragraphe 1, pour lesquelles la demande de données de santé est présentée;

c) une description des données de santé électroniques demandées, de leur format et des sources de ces données, si possible;

d) une description du contenu statistique;

e) une description des garanties prévues pour empêcher toute utilisation abusive des données de santé électroniques demandées;

f) une description de la manière dont le traitement serait conforme à l'article 6, paragraphe 1, du règlement (UE) 2016/679 ou à l'article 5, paragraphe 1, et à l'article 10, paragraphe 2, du règlement (UE) 2018/1725;

g) lorsque le demandeur de données de santé a l'intention de faire usage d'une exception au titre de l'article 71, paragraphe 4, la justification requise à cet égard par le droit national en vertu dudit article.

3. L'organisme responsable de l'accès aux données de santé évalue si la demande de données de santé est complète et tient compte des risques visés à l'article 68, paragraphe 2.

4. L'organisme responsable de l'accès aux données de santé évalue la demande de données de santé dans un délai de trois mois à compter de la réception de la demande et, si possible, fournit ensuite la réponse à l'utilisateur de données de santé dans un délai supplémentaire de trois mois.

Article 70

Modèles pour soutenir l'accès aux données de santé électroniques à des fins d'utilisation secondaire

Au plus tard le 26 mars 2027, la Commission, par voie d'actes d'exécution, établit les modèles pour la demande d'accès aux données de santé, pour l'autorisation de traitement de données et pour la demande de données de santé visées, respectivement, aux articles 67, 68 et 69. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 71

Droit de refuser le traitement des données de santé électroniques à caractère personnel à des fins d'utilisation secondaire

1. Les personnes physiques ont le droit de refuser à tout moment et sans motif le traitement des données de santé électroniques à caractère personnel les concernant à des fins d'utilisation secondaire au titre du présent règlement. L'exercice de ce droit est réversible.

2. Les États membres prévoient un mécanisme de refus accessible et facilement compréhensible permettant d'exercer le droit établi au paragraphe 1, par lequel les personnes physiques peuvent exprimer explicitement leur volonté que leurs données de santé électroniques à caractère personnel ne soient pas traitées à des fins d'utilisation secondaire.

3. Dès que des personnes physiques ont exercé leur droit de refus, et lorsque des données de santé électroniques à caractère personnel les concernant peuvent être identifiées dans un ensemble de données, les données de santé électroniques à caractère personnel concernant ces personnes physiques ne sont pas mises à disposition ou traitées d'une autre manière en vertu d'autorisations de traitement de données délivrées en vertu de l'article 68 ou de demandes de données de santé approuvées en vertu de l'article 69 après que les personnes physiques ont exercé leur droit de refus.

Le premier alinéa du présent paragraphe n'affecte pas le traitement à des fins d'utilisation secondaire des données de santé électroniques à caractère personnel concernant ces personnes physiques en vertu d'autorisations de traitement de données ou de demandes de données de santé qui ont été délivrées ou approuvées avant que les personnes physiques aient exercé leur droit de refus.

4. Par dérogation au droit de refus prévu au paragraphe 1, un État membre peut prévoir, dans son droit national, un mécanisme permettant de mettre à disposition des données pour lesquelles un droit de refus a été exercé, à condition que toutes les conditions suivantes soient remplies:

a) la demande d'accès aux données de santé ou la demande de données de santé est présentée par un organisme du secteur public ou une institution, un organe ou un organisme de l'Union ayant pour mandat d'accomplir des tâches dans le domaine de la santé publique, ou par une autre entité chargée d'accomplir des tâches publiques dans le domaine de la santé publique, ou agissant au nom d'une autorité publique ou mandatée par celle-ci, et le traitement est nécessaire pour l'une des finalités suivantes:

   i) les finalités visées à l'article 53, paragraphe 1, points a), b) et c);

   ii) la recherche scientifique pour des motifs importants d'intérêt public;

b) ces données ne peuvent être obtenues par d'autres moyens en temps utile et de manière efficace à des conditions équivalentes;

c) le demandeur de données de santé a fourni la justification visée à l'article 68, paragraphe 1, point g), ou à l'article 69, paragraphe 2, point g).

Le droit national prévoyant un tel mécanisme contient des mesures spécifiques et appropriées visant à protéger les droits fondamentaux et les données à caractère personnel des personnes physiques.

Lorsqu'un État membre prévoit dans son droit national la possibilité de demander l'accès à des données pour lesquelles un droit de refus a été exercé et que les conditions visées au premier alinéa du présent paragraphe sont remplies, ces données peuvent être incluses dans le cadre de l'accomplissement des tâches visées à l'article 57, paragraphe 1, points a), i), a), iii), et b).

5. Les règles relatives à tout mécanisme visant à mettre en œuvre des exceptions prévu au paragraphe 4 par dérogation au paragraphe 1 respectent l'essence des droits et libertés fondamentaux et constituent une mesure nécessaire et proportionnée dans une société démocratique pour réaliser des finalités d'intérêt public dans le domaine d'objectifs scientifiques et sociétaux légitimes.

6. Tout traitement effectué au titre d'un mécanisme visant à mettre en œuvre des exceptions prévu au paragraphe 4 du présent article respecte les exigences du présent chapitre, notamment l'interdiction de réidentifier ou de tenter de réidentifier des personnes physiques conformément à l'article 61, paragraphe 3. Toute mesure législative prévoyant, dans le droit national, un mécanisme visé au paragraphe 4 du présent article contient des dispositions spécifiques en matière de sécurité et de protection des droits des personnes physiques.

7. Les États membres notifient sans retard à la Commission les dispositions de leur droit national qu'ils adoptent en vertu du paragraphe 4, de même que toute modification ultérieure les concernant.

8. Lorsque les finalités du traitement des données de santé électroniques à caractère personnel par un détenteur de données de santé ne nécessitent pas ou ne nécessitent plus l'identification d'une personne concernée par le responsable du traitement, ce détenteur de données de santé n'est pas tenu de conserver, d'acquérir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le droit de refus prévu par le présent article.

Article 72

Procédure simplifiée d'accès aux données de santé électroniques d'un détenteur de données de santé de confiance

1. Lorsqu'un organisme responsable de l'accès aux données de santé reçoit une demande d'accès aux données de santé en vertu de l'article 67 ou une demande de données de santé en vertu de l'article 69 qui ne couvre que les données de santé électroniques détenues par un détenteur de données de santé de confiance désigné conformément au paragraphe 2 du présent article, la procédure prévue aux paragraphes 4 à 6 du présent article s'applique.

2. Les États membres peuvent établir une procédure par laquelle les détenteurs de données de santé peuvent demander à être désignés comme détenteurs de données de santé de confiance, à condition que les détenteurs de données de santé remplissent les conditions suivantes:

a) ils peuvent donner accès aux données de santé au moyen d'un environnement de traitement sécurisé conforme à l'article 73;

b) ils disposent de l'expertise nécessaire pour évaluer les demandes d'accès aux données de santé et les demandes de données de santé;

c) ils fournissent les garanties nécessaires quant au respect du présent règlement.

Les États membres désignent des détenteurs de données de santé de confiance après évaluation du respect de ces conditions par l'organisme responsable de l'accès aux données de santé concerné.

Les États membres établissent une procédure pour vérifier régulièrement si le détenteur de données de santé de confiance continue de remplir ces conditions.

Les organismes responsables de l'accès aux données de santé mentionnent les détenteurs de données de santé de confiance dans le catalogue des ensembles de données visé à l'article 77.

3. Les demandes d'accès aux données de santé et les demandes de données de santé visées au paragraphe 1 sont présentées à l'organisme responsable de l'accès aux données de santé, qui peut les transmettre au détenteur de données de santé de confiance concerné.

4. À la suite de la réception d'une demande d'accès aux données de santé ou d'une demande de données de santé en vertu du paragraphe 3 du présent article, le détenteur de données de santé de confiance évalue la demande d'accès aux données de santé ou la demande de données de santé au regard des critères énumérés à l'article 68, paragraphes 1 et 2, ou à l'article 69, paragraphes 2 et 3, selon le cas.

5. Le détenteur de données de santé de confiance soumet l'évaluation qu'il effectue en vertu du paragraphe 4, accompagnée d'une proposition de décision, à l'organisme responsable de l'accès aux données de santé dans un délai de deux mois à compter de la réception de la demande d'accès aux données de santé ou de la demande de données de santé émanant de l'organisme responsable de l'accès aux données de santé. Dans les deux mois à compter de la réception de l'évaluation, l'organisme responsable de l'accès aux données de santé prend une décision sur la demande d'accès aux données de santé ou la demande de données de santé. L'organisme responsable de l'accès aux données de santé n'est pas lié par la proposition soumise par le détenteur de données de santé de confiance.

6. À la suite de la décision de l'organisme responsable de l'accès aux données de santé de délivrer l'autorisation de traitement de données ou d'approuver la demande de données de santé, le détenteur de données de santé de confiance accomplit les tâches visées à l'article 57, paragraphe 1, points a), i), et b).

7. Le service d'accès aux données de santé de l'Union visé à l'article 56 peut désigner en tant que détenteurs de données de santé de confiance des détenteurs de données de santé qui sont des institutions, organes ou organismes de l'Union qui remplissent les conditions prévues au paragraphe 2, premier alinéa, points a), b) et c), du présent article. Dans ce cas, le paragraphe 2, troisième et quatrième alinéas, et les paragraphes 3 à 6 du présent article s'appliquent mutatis mutandis.

Article 73

Environnement de traitement sécurisé

1. Les organismes responsables de l'accès aux données de santé ne donnent accès aux données de santé électroniques en vertu d'une autorisation de traitement de données qu'au moyen d'un environnement de traitement sécurisé, qui est soumis à des mesures techniques et organisationnelles et à des exigences en matière de sécurité et d'interopérabilité. L'environnement de traitement sécurisé respecte notamment les mesures de sécurité suivantes:

a) restreindre aux personnes physiques autorisées énumérées dans l'autorisation de traitement de données délivrée en vertu de l'article 68 l'accès à l'environnement de traitement sécurisé;

b) réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées de données de santé électroniques hébergées dans l'environnement de traitement sécurisé par des mesures techniques et organisationnelles de pointe;

c) restreindre à un nombre limité d'individus identifiables autorisés l'introduction de données de santé électroniques et l'inspection, la modification ou la suppression de données de santé électroniques hébergées dans l'environnement de traitement sécurisé;

d) veiller à ce que les utilisateurs de données de santé n'aient accès qu'aux données de santé électroniques couvertes par leur autorisation de traitement de données, au moyen d'identifiants individuels et uniques et de modes d'accès confidentiels uniquement;

e) tenir des registres identifiables d'accès à l'environnement de traitement sécurisé et des activités qui sont menées dans cet environnement pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement; les registres d'accès sont conservés pendant au moins un an;

f) veiller à la conformité et contrôler les mesures de sécurité visées au présent paragraphe, afin d'atténuer les menaces potentielles pour la sécurité.

2. Les organismes responsables de l'accès aux données de santé veillent à ce que les données de santé électroniques provenant des détenteurs de données de santé au format défini dans l'autorisation de traitement de données puissent être téléversées par ces détenteurs de données de santé et que l'utilisateur de données de santé puisse y avoir accès dans un environnement de traitement sécurisé.

Les organismes responsables de l'accès aux données de santé examinent les données de santé électroniques contenues dans une demande de téléchargement afin de veiller à ce que les utilisateurs de données de santé ne puissent télécharger que des données de santé électroniques à caractère non personnel, notamment des données de santé électroniques dans un format statistique anonymisé, à partir de l'environnement de traitement sécurisé.

3. Les organismes responsables de l'accès aux données de santé veillent à ce que les environnements de traitement sécurisés fassent régulièrement l'objet d'audits, y compris par des tiers, et prennent des mesures correctives pour pallier les lacunes, les risques ou les vulnérabilités constatés lors de ces audits dans les environnements de traitement sécurisés.

4. Lorsque des organisations altruistes en matière de données reconnues visées au chapitre IV du règlement (UE) 2022/868 traitent des données de santé électroniques à caractère personnel au moyen d'un environnement de traitement sécurisé, ledit environnement respecte également les mesures de sécurité énoncées au paragraphe 1, points a) à f), du présent article.

5. Au plus tard le 26 mars 2027, la Commission fixe, par voie d'actes d'exécution, les exigences techniques et organisationnelles, ainsi que les exigences en matière de sécurité de l'information, de confidentialité, de protection des données et d'interopérabilité applicables aux environnements de traitement sécurisés, y compris en ce qui concerne les caractéristiques techniques et les outils dont peut disposer l'utilisateur de données de santé dans les environnements de traitement sécurisés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 74

Responsabilité du traitement

1. Le détenteur de données de santé est réputé être le responsable du traitement pour la mise à la disposition de l'organisme responsable de l'accès aux données de santé des données de santé électroniques à caractère personnel demandées en vertu de l'article 60, paragraphe 1.

L'organisme responsable de l'accès aux données de santé est réputé être le responsable du traitement des données de santé électroniques à caractère personnel lorsqu'il accomplit ses tâches en vertu du présent règlement.

Nonobstant le deuxième alinéa du présent paragraphe, l'organisme responsable de l'accès aux données de santé est réputé agir en qualité de sous-traitant pour le compte de l'utilisateur de données de santé agissant en tant que responsable du traitement en ce qui concerne le traitement des données de santé électroniques à caractère personnel en vertu d'une autorisation de traitement de données délivrée au titre de l'article 68 dans l'environnement de traitement sécurisé lorsqu'il fournit des données au moyen de cet environnement ou en ce qui concerne le traitement de telles données en vertu d'une demande de données de santé approuvée au titre de l'article 69 pour qu'une réponse soit générée.

2. Dans les situations visées à l'article 72, paragraphe 6, le détenteur de données de santé de confiance est réputé être le responsable du traitement en ce qui concerne le traitement des données de santé électroniques à caractère personnel lié à la fourniture de données de santé électroniques à l'utilisateur de données de santé en vertu d'une autorisation de traitement de données ou d'une demande de données de santé. Le détenteur de données de santé de confiance est réputé agir en tant que sous-traitant pour le compte de l'utilisateur de données de santé lorsqu'il fournit des données au moyen d'un environnement de traitement sécurisé.

3. La Commission peut, par voie d'actes d'exécution, établir un modèle pour les accords entre les responsables du traitement et les sous-traitants dans le cadre des paragraphes 1 et 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

SECTION 4

Infrastructure transfrontière pour l'utilisation secondaire

Article 75

DonnéesDeSanté@UE (HealthData@EU)

1. Chaque État membre désigne un point de contact national pour l'utilisation secondaire. Ce point de contact national pour l'utilisation secondaire est un portail organisationnel et technique, qui permet la mise à disposition des données de santé électroniques à des fins d'utilisation secondaire dans un contexte transfrontière, et qui est responsable de cette mise à disposition. Le point de contact national pour l'utilisation secondaire peut être l'organisme responsable de l'accès aux données de santé désigné comme coordonnateur visé à l'article 55, paragraphe 1. Chaque État membre communique à la Commission le nom et les coordonnées du point de contact national pour l'utilisation secondaire au plus tard le 26 mars 2027. La Commission et les États membres mettent ces informations à la disposition du public.

2. Le service d'accès aux données de santé de l'Union fait office de point de contact des institutions, organes et organismes de l'Union pour l'utilisation secondaire et est responsable de la mise à disposition des données de santé électroniques à des fins d'utilisation secondaire.

3. Les points de contact nationaux pour l'utilisation secondaire visés au paragraphe 1 et le service d'accès aux données de santé de l'Union visé au paragraphe 2 se connectent à l'infrastructure transfrontière pour l'utilisation secondaire, à savoir DonnéesDeSanté@UE (HealthData@EU). Les points de contact nationaux pour l'utilisation secondaire et le service d'accès aux données de santé de l'Union facilitent l'accès transfrontière aux données de santé électroniques à des fins d'utilisation secondaire de différents participants autorisés à DonnéesDeSanté@UE (HealthData@EU). Les points de contact nationaux pour l'utilisation secondaire coopèrent étroitement entre eux et avec la Commission.

4. Les infrastructures de recherche dans le domaine de la santé ou les infrastructures similaires dont le fonctionnement est fondé sur le droit de l'Union et qui favorisent l'utilisation de données de santé électroniques à des fins de recherche, d'élaboration de politiques, de statistiques, de sécurité des patients ou de réglementation peuvent devenir des participants autorisés à DonnéesDeSanté@UE (HealthData@EU) et s'y connecter.

5. Les pays tiers ou les organisations internationales peuvent devenir des participants autorisés à DonnéesDeSanté@UE (HealthData@EU) lorsqu'ils respectent les règles du présent chapitre et qu'ils donnent aux utilisateurs de données de santé situés dans l'Union l'accès, selon des modalités et à des conditions équivalentes, aux données de santé électroniques dont disposent leurs organismes responsables de l'accès aux données de santé, sous réserve du respect du chapitre V du règlement (UE) 2016/679.

La Commission peut déterminer, par voie d'actes d'exécution, qu'un point de contact national pour une utilisation secondaire d'un pays tiers ou un système établi à l'échelon international par une organisation internationale respecte les exigences de DonnéesDeSanté@UE (HealthData@EU) aux fins de l'utilisation secondaire des données de santé, respecte le présent chapitre et donne aux utilisateurs de données de santé situés dans l'Union l'accès aux données de santé électroniques auxquelles il a accès, selon des modalités et à des conditions équivalentes à celles de DonnéesDeSanté@UE (HealthData@EU). Le respect de ces exigences juridiques, organisationnelles, techniques et de sécurité, y compris des exigences applicables aux environnements de traitement sécurisés prévus à l'article 73, est vérifié sous le contrôle de la Commission. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2. La Commission met la liste des actes d'exécution adoptés en vertu du présent paragraphe à la disposition du public.

6. Chaque point de contact national pour l'utilisation secondaire et chaque participant autorisé à DonnéesDeSanté@UE (HealthData@EU) acquiert la capacité technique requise pour se connecter et participer à DonnéesDeSanté@UE (HealthData@EU). Ils se conforment aux exigences et aux spécifications techniques nécessaires pour exploiter DonnéesDeSanté@UE (HealthData@EU) et pour pouvoir s'y connecter.

7. Les États membres et la Commission mettent en place DonnéesDeSanté@UE (HealthData@EU) afin de soutenir et de faciliter l'accès transfrontière aux données de santé électroniques à des fins d'utilisation secondaire, en assurant la connexion entre les points de contact nationaux pour l'utilisation secondaire et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU) ainsi que la plateforme centrale visée au paragraphe 8.

8. La Commission met au point, déploie et exploite une plateforme centrale pour DonnéesDeSanté@UE (HealthData@EU) en fournissant les services informatiques nécessaires afin de soutenir et de faciliter l'échange d'informations entre les organismes responsables de l'accès aux données de santé dans le cadre de DonnéesDeSanté@UE (HealthData@EU). La Commission ne traite les données de santé électroniques que pour le compte des responsables du traitement, en tant que sous-traitant.

9. À la demande d'au moins deux points de contact nationaux pour l'utilisation secondaire, la Commission peut prévoir un environnement de traitement sécurisé qui respecte les exigences de l'article 73 pour les données provenant de plus d'un État membre. Lorsqu'au moins deux points de contact nationaux pour l'utilisation secondaire ou participants autorisés à DonnéesDeSanté@UE (HealthData@EU) introduisent des données de santé électroniques dans l'environnement de traitement sécurisé géré par la Commission, ils sont les responsables conjoints du traitement, et la Commission est le sous-traitant aux fins du traitement des données dans cet environnement.

10. Les points de contact nationaux pour l'utilisation secondaire agissent en qualité de responsables conjoints des opérations de traitement effectuées dans DonnéesDeSanté@UE (HealthData@EU) auxquelles ils sont associés, et la Commission agit en qualité de sous-traitant pour le compte de ces points de contact nationaux pour l'utilisation secondaire, sans que cela n'ait d'incidence sur les tâches des organismes responsables de l'accès aux données de santé avant et après ces opérations de traitement.

11. Les États membres et la Commission s'efforcent de garantir que DonnéesDeSanté@UE (HealthData@EU) est interopérable avec les autres espaces européens communs des données pertinents visés dans les règlements (UE) 2022/868 et (UE) 2023/2854.

12. Au plus tard le 26 mars 2027, la Commission, par voie d'actes d'exécution, établit:

a) les exigences, les spécifications techniques et l'architecture informatique de DonnéesDeSanté@UE (HealthData@EU), qui assurent un niveau optimal de sécurité des données, de confidentialité et de protection des données de santé électroniques dans DonnéesDeSanté@UE (HealthData@EU);

b) les conditions et les contrôles de conformité exigés pour pouvoir adhérer et rester connecté à DonnéesDeSanté@UE (HealthData@EU), ainsi que les conditions de déconnexion temporaire ou d'exclusion définitive de DonnéesDeSanté@UE (HealthData@EU), y compris les dispositions spécifiques en cas de faute grave ou de violations répétées;

c) les critères minimaux que doivent remplir les points de contact nationaux pour l'utilisation secondaire et les participants autorisés à DonnéesDeSanté@UE (HealthData@EU);

d) les responsabilités des responsables du traitement et des sous-traitants participant à DonnéesDeSanté@UE (HealthData@EU);

e) les responsabilités des responsables du traitement et des sous-traitants en ce qui concerne l'environnement de traitement sécurisé géré par la Commission;

f) les spécifications communes applicables à l'architecture de DonnéesDeSanté@UE (HealthData@EU) et à son interopérabilité avec d'autres espaces européens communs des données.

Les actes d'exécution visés au premier alinéa du présent paragraphe sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

13. En cas de résultat positif d'un contrôle de conformité visé au paragraphe 5 du présent article, la Commission peut, par voie d'actes d'exécution, prendre des décisions visant à connecter des participants autorisés individuels à DonnéesDeSanté@UE (HealthData@EU). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 76

Accès aux registres ou bases de données transfrontières de données de santé électroniques à des fins d'utilisation secondaire

1. Dans le cas de registres et de bases de données transfrontières, l'organisme responsable de l'accès aux données de santé auprès duquel le détenteur de données de santé pour le registre ou la base de données spécifique est enregistré est compétent pour statuer sur les demandes d'accès aux données de santé visant à donner accès aux données de santé électroniques en vertu d'une autorisation de traitement de données. Lorsque les registres ou les bases de données ont des responsables conjoints du traitement, l'organisme responsable de l'accès aux données de santé qui statue sur les demandes d'accès aux données de santé à utiliser pour donner accès aux données de santé électroniques est l'organisme responsable de l'accès aux données de santé de l'État membre dans lequel un des responsables conjoints du traitement est établi.

2. Lorsque des registres ou des bases de données d'un certain nombre d'États membres s'organisent en un réseau unique de registres ou de bases de données à l'échelle de l'Union, les registres ou bases de données associés peuvent désigner un coordonnateur pour assurer la fourniture de données du réseau de registres ou de bases de données à des fins d'utilisation secondaire. L'organisme responsable de l'accès aux données de santé de l'État membre dans lequel est établi le coordonnateur du réseau est compétent pour statuer sur les demandes d'accès aux données de santé à utiliser pour donner accès aux données de santé électroniques pour le réseau de registres ou de bases de données.

SECTION 5

Qualité et utilité des données de santé à des fins d'utilisation secondaire

Article 77

Description de l'ensemble de données et catalogue des ensembles de données

1. Les organismes responsables de l'accès aux données de santé fournissent, au moyen d'un catalogue des ensembles de données normalisé, accessible au public et lisible par machine, une description sous la forme de métadonnées, des ensembles de données disponibles et de leurs caractéristiques. La description de chaque ensemble de données comprend des informations concernant la source, la portée, les caractéristiques principales et la nature des données de santé électroniques dans l'ensemble de données et les conditions de mise à disposition de ces données.

2. Les descriptions des ensembles de données figurant dans le catalogue des ensembles de données national sont disponibles, dans au moins une langue officielle de l'Union. Le catalogue des ensembles de données pour les institutions, organes et organismes de l'Union fourni par le service d'accès aux données de santé de l'Union est disponible dans toutes les langues officielles de l'Union.

3. Le catalogue des ensembles de données est mis à la disposition des points d'information uniques établis ou désignés en vertu de l'article 8 du règlement (UE) 2022/868.

4. Au plus tard le 26 mars 2027, la Commission détermine, par voie d'actes d'exécution, les éléments minimaux que les détenteurs de données de santé doivent fournir concernant les ensembles de données et les caractéristiques de ces éléments. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 78

Label de qualité et d'utilité des données

1. Les ensembles de données mis à disposition par l'intermédiaire des organismes responsables de l'accès aux données de santé peuvent être accompagnés d'un label de qualité et d'utilité des données de l'Union apposé par les détenteurs de données de santé.

2. Les ensembles de données contenant des données de santé électroniques collectées et traitées avec le soutien d'un financement public national ou de l'Union sont accompagnés d'un label de qualité et d'utilité des données couvrant les éléments énoncés au paragraphe 3.

3. Le label de qualité et d'utilité des données couvre, le cas échéant, les éléments suivants:

a) pour la documentation des données: les métadonnées, la documentation d'appui, le dictionnaire de données, le format et les normes utilisés, la source des données et, le cas échéant, le modèle de données;

b) pour l'évaluation de la qualité technique: l'exhaustivité, l'unicité, l'exactitude, la validité, l'actualité et la cohérence des données;

c) pour les processus de gestion de la qualité des données: le niveau de maturité des processus de gestion de la qualité des données, dont les processus d'examen et d'audit, et l'examen des biais;

d) pour l'évaluation de la couverture: la période, la population couverte et, le cas échéant, la représentativité de la population échantillonnée et la période moyenne dans laquelle une personne physique apparaît dans un ensemble de données;

e) pour les informations sur l'accès et la fourniture: le délai entre la collecte des données de santé électroniques et leur ajout à l'ensemble de données et le temps nécessaire pour la fourniture de données de santé électroniques à la suite de la délivrance d'une autorisation de traitement de données ou de l'approbation d'une demande de données de santé;

f) pour les informations sur les modifications de données: la fusion et l'ajout de données à un ensemble de données existant, les liens avec d'autres ensembles de données.

4. Lorsqu'un organisme responsable de l'accès aux données de santé a des raisons de croire qu'un label de qualité et d'utilité des données pourrait être inexact, il évalue si l'ensemble de données couvert par le label satisfait aux exigences de qualité faisant partie des éléments du label de qualité et d'utilité des données visés au paragraphe 3 et, dans le cas où l'ensemble de données ne satisfait pas aux exigences de qualité, révoque le label.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier le présent règlement en modifiant les éléments que doit couvrir le label de qualité et d'utilité des données prévus au paragraphe 3 du présent article, ou en ajoutant ou en supprimant de tels éléments.

6. Au plus tard le 26 mars 2027, la Commission détermine, par voie d'actes d'exécution, les caractéristiques visuelles et les spécifications techniques du label de qualité et d'utilité des données, sur la base des éléments visés au paragraphe 3 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2, du présent règlement. Ces actes d'exécution tiennent compte des exigences énoncées à l'article 10 du règlement (UE) 2024/1689 et de toutes spécifications communes ou normes harmonisées adoptées qui soutiennent ces exigences, le cas échéant.

Article 79

Catalogue des ensembles de données de l'UE

1. La Commission établit un catalogue des ensembles de données de l'UE mettant en relation les catalogues des ensembles de données nationaux établis par les organismes responsables de l'accès aux données de santé dans chaque État membre ainsi que les catalogues des ensembles de données des participants autorisés à DonnéesDeSanté@UE (HealthData@EU).

2. Le catalogue des ensembles de données de l'UE, les catalogues des ensembles de données nationaux et les catalogues des ensembles de données des participants autorisés à DonnéesDeSanté@UE (HealthData@EU) sont rendus publics.

Article 80

Spécifications minimales applicables aux ensembles de données ayant une incidence majeure

La Commission peut, par voie d'actes d'exécution, déterminer les spécifications minimales applicables aux ensembles de données ayant une incidence majeure sur l'utilisation secondaire, en tenant compte des infrastructures, normes, lignes directrices et recommandations existantes de l'Union. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

SECTION 6

Réclamations

Article 81

Droit d'introduire une réclamation auprès d'un organisme responsable de l'accès aux données de santé

1. Sans préjudice de tout autre recours administratif ou juridictionnel, les personnes physiques et les personnes morales ont le droit d'introduire une réclamation en lien avec les dispositions du présent chapitre, individuellement ou, le cas échéant, collectivement, auprès d'un organisme responsable de l'accès aux données de santé, pour autant que leurs droits ou intérêts soient lésés.

2. L'organisme responsable de l'accès aux données de santé auprès duquel la réclamation a été introduite informe l'auteur de la réclamation des progrès réalisés dans le traitement de la réclamation et de la décision prise au sujet de la réclamation.

3. Les organismes responsables de l'accès aux données de santé mettent à disposition des outils facilement accessibles pour introduire des réclamations.

4. Lorsque la réclamation concerne les droits de personnes physiques en vertu de l'article 71 du présent règlement, la réclamation est transmise à l'autorité de contrôle compétente au titre du règlement (UE) 2016/679. L'organisme responsable de l'accès aux données de santé compétent fournit les informations nécessaires dont elle dispose à cette autorité de contrôle en vertu du règlement (UE) 2016/679 afin de faciliter l'évaluation et l'enquête portant sur la réclamation.

CHAPITRE V

AUTRES ACTIONS

Article 82

Renforcement des capacités

La Commission soutient la mise en commun des bonnes pratiques et de l'expertise en vue de renforcer la capacité au sein des États membres à développer les systèmes de santé numériques en ce qui concerne l'utilisation primaire et l'utilisation secondaire, en tenant compte des situations spécifiques des différentes catégories de parties prenantes concernées. Afin de soutenir le renforcement des capacités, la Commission, en étroite collaboration et concertation avec les États membres, élabore des indicateurs d'autoévaluation pour l'utilisation primaire et l'utilisation secondaire.

Article 83

Programmes de formation et information des professionnels de la santé

1. Les États membres élaborent et mettent en œuvre des programmes de formation pour les professionnels de la santé, ou leur donnent accès à de tels programmes, et leur donnent accès à des informations, afin qu'ils comprennent et remplissent efficacement leur rôle en ce qui concerne l'utilisation primaire des données de santé électroniques et l'accès à ces données, notamment en lien avec les articles 11, 13 et 16. La Commission soutient les États membres à cet égard.

2. Les programmes de formation et les informations sont accessibles et abordables pour tous les professionnels de la santé, sans préjudice de l'organisation des systèmes de soins de santé au niveau national.

Article 84

Maîtrise des outils de santé numérique et accès à la santé numérique

1. Les États membres promeuvent et soutiennent la maîtrise des outils de santé numérique et le développement des compétences et aptitudes pertinentes pour les patients. La Commission soutient les États membres à cet égard. Les campagnes ou programmes de sensibilisation visent en particulier à informer les patients et le grand public sur l'utilisation primaire et l'utilisation secondaire dans le cadre de l'EEDS, y compris sur les droits qui en découlent, ainsi que sur les avantages, les risques et les bienfaits potentiels pour la science et la société de l'utilisation primaire et de l'utilisation secondaire.

2. Les campagnes et programmes de sensibilisation visés au paragraphe 1 sont adaptés aux besoins de groupes spécifiques et sont développés, réexaminés et, le cas échéant, mis à jour.

3. Les États membres promeuvent l'accès à l'infrastructure nécessaire à la gestion efficace des données de santé électroniques des personnes physiques, tant à des fins d'utilisation primaire que d'utilisation secondaire.

Article 85

Exigences supplémentaires en matière de marchés publics et de financement de l'Union

1. Les pouvoirs adjudicateurs, dont les autorités de santé numérique et les organismes responsables de l'accès aux données de santé, ainsi que les institutions, organes et organismes de l'Union, font référence aux spécifications techniques, aux normes et aux profils applicables visés aux articles 15, 23, 36, 73, 75 et 78 pour les procédures de marchés publics et lors de la formulation de leurs dossiers d'appels d'offres ou d'appels à propositions, ainsi que lors de la fixation des conditions d'obtention d'un financement de l'Union concernant le présent règlement, y compris les conditions favorisantes pour ce qui est des Fonds structurels et des fonds de cohésion.

2. Les critères d'obtention d'un financement de l'Union tiennent compte des exigences élaborées dans le cadre des chapitres II, III et IV.

Article 86

Conservation des données de santé électroniques à caractère personnel à des fins d'utilisation primaire

Conformément aux principes généraux du droit de l'Union, qui comprennent les droits fondamentaux consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, les États membres assurent la mise en place d'un niveau particulièrement élevé de protection et de sécurité lors du traitement des données de santé électroniques à caractère personnel à des fins d'utilisation primaire, au moyen de mesures techniques et organisationnelles appropriées. À cet égard, le présent règlement ne fait pas obstacle à ce que le droit national, compte tenu du contexte national, exige que, dans les cas où des données de santé électroniques à caractère personnel sont traitées par des prestataires de soins de santé aux fins de la fourniture de soins de santé ou par les points de contact nationaux pour la santé numérique connectés à MaSanté@UE (MyHealth@EU), la conservation des données de santé électroniques à caractère personnel visées à l'article 14 du présent règlement à des fins d'utilisation primaire soit situé dans l'Union, en conformité avec le droit de l'Union et les engagements internationaux.

Article 87

Conservation des données de santé électroniques à caractère personnel par les organismes responsables de l'accès aux données de santé et environnements de traitement sécurisés

1. Les organismes responsables de l'accès aux données de santé, les détenteurs de données de santé de confiance et le service d'accès aux données de santé de l'Union conservent et traitent les données de santé électroniques à caractère personnel dans l'Union lorsqu'ils effectuent des opérations de pseudonymisation, d'anonymisation et toute autre opération de traitement de données à caractère personnel visée aux articles 67 à 72, au moyen d'environnements de traitement sécurisés au sens de l'article 73 et de l'article 75, paragraphe 9, ou au moyen de DonnéesDeSanté@UE (HealthData@EU). Cette exigence s'applique à toute entité accomplissant ces tâches au nom de ces organismes, ces détenteurs ou ce service.

2. Par dérogation au paragraphe 1 du présent article, les données visées audit paragraphe peuvent être conservées et traitées dans un pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers lorsque ce pays, territoire ou secteur est couvert par une décision d'adéquation adoptée en vertu de l'article 45 du règlement (UE) 2016/679.

Article 88

Transfert de données électroniques à caractère non personnel vers un pays tiers

1. Les données de santé électroniques à caractère non personnel mises à la disposition d'un utilisateur de données de santé dans un pays tiers par les organismes responsables de l'accès aux données de santé au titre d'une autorisation de traitement de données délivrée en vertu de l'article 68 du présent règlement ou d'une demande de données approuvée en vertu de l'article 69 du présent règlement, ou mises à la disposition de participants autorisés dans un pays tiers ou d'une organisation internationale, et fondées sur les données de santé électroniques d'une personne physique qui relèvent de l'une des catégories visées à l'article 51 du présent règlement, sont considérées comme hautement sensibles au sens de l'article 5, paragraphe 13, du règlement (UE) 2022/868, lorsque le transfert de telles données électroniques à caractère non personnel vers des pays tiers présente un risque de réidentification par des moyens allant au-delà de ceux raisonnablement susceptibles d'être utilisés, compte tenu en particulier du nombre limité de personnes physiques auxquelles ces données se rapportent, du fait que ces personnes physiques sont géographiquement dispersées ou des évolutions technologiques attendues dans un avenir proche.

2. Les mesures de protection pour les catégories de données visées au paragraphe 1 du présent article sont détaillées dans un acte délégué comme visé à l'article 5, paragraphe 13, du règlement (UE) 2022/868.

Article 89

Accès international des autorités publiques aux données de santé électroniques à caractère non personnel

1. Les autorités de santé numérique, les organismes responsables de l'accès aux données de santé, les participants autorisés aux infrastructures transfrontières prévues aux articles 23 et 75 et les utilisateurs de données de santé prennent toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris des arrangements contractuels, afin d'empêcher le transfert de données de santé électroniques à caractère non personnel détenues dans l'Union vers un pays tiers ou une organisation internationale, ou l'accès des autorités publiques d'un pays tiers à de telles données, lorsque ce transfert risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné.

2. Toute décision d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'une autorité de santé numérique, d'un organisme responsable de l'accès aux données de santé ou d'utilisateurs de données de santé qu'ils transfèrent des données de santé électroniques à caractère non personnel relevant du champ d'application du présent règlement détenues dans l'Union, ou qu'ils donnent accès à de telles données, ne sont reconnues ou exécutoires de quelque manière que ce soit que si elles sont fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union, ou sur tout accord de ce type entre le pays tiers demandeur et un État membre.

3. En l'absence d'un accord international comme visé au paragraphe 2, lorsqu'une autorité de santé numérique, un organisme responsable de l'accès aux données de santé ou un utilisateur de données de santé est destinataire d'une décision d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers, exigeant qu'ils transfèrent des données à caractère non personnel relevant du champ d'application du présent règlement détenues dans l'Union, ou qu'ils donnent accès à de telles données, et lorsque le respect d'une telle décision risquerait de mettre le destinataire en conflit avec le droit de l'Union ou avec le droit national de l'État membre concerné, le transfert de ces données vers cette juridiction ou cette autorité administrative d'un pays tiers n'a lieu ou l'accès à ces données par cette même juridiction ou autorité n'est donné que si:

a) le système juridique du pays tiers exige que les motifs et la proportionnalité d'une telle décision soient exposés et que cette décision revête un caractère spécifique, par exemple en établissant un lien suffisant avec certaines personnes suspectées ou avec des infractions;

b) l'objection motivée du destinataire fait l'objet d'un examen par une juridiction compétente du pays tiers; et

c) la juridiction compétente du pays tiers qui rend la décision ou contrôle la décision d'une autorité administrative est habilitée par le droit national du pays tiers à prendre dûment en compte les intérêts juridiques concernés du fournisseur des données protégés par le droit de l'Union ou par le droit national de l'État membre concerné.

4. Si les conditions énoncées au paragraphe 2 ou 3 sont remplies, une autorité de santé numérique, un organisme responsable de l'accès aux données de santé ou une organisation altruiste en matière de données fournit le volume minimal de données admissible en réponse à une demande, sur la base d'une interprétation raisonnable de la demande.

5. Les autorités de santé numérique, les organismes responsables de l'accès aux données de santé et les utilisateurs de données de santé informent le détenteur de données de l'existence d'une demande d'accès à ses données émanant d'une autorité administrative d'un pays tiers avant de donner suite à cette demande, sauf si la demande sert des fins répressives et aussi longtemps que donner suite à cette demande est nécessaire pour préserver l'efficacité de l'action répressive.

Article 90

Conditions supplémentaires pour le transfert de données de santé électroniques à caractère personnel vers un pays tiers ou une organisation internationale

Le transfert de données de santé électroniques à caractère personnel vers un pays tiers ou une organisation internationale est octroyé conformément au chapitre V du règlement (UE) 2016/679. Les États membres peuvent maintenir ou introduire d'autres conditions relatives à l'accès international aux données de santé électroniques à caractère personnel et au transfert de ces données, y compris des limitations, conformément à l'article 9, paragraphe 4, du règlement (UE) 2016/679, en plus des exigences fixées à l'article 24, paragraphe 3, et à l'article 75, paragraphe 5, du présent règlement et au chapitre V du règlement (UE) 2016/679.

Article 91

Demandes d'accès aux données de santé et demandes de données de santé émanant de pays tiers

1. Sans préjudice des articles 67, 68 et 69, les demandes d'accès aux données de santé et les demandes de données de santé présentées par un demandeur de données de santé établi dans un pays tiers sont prises en considération par les organismes responsables de l'accès aux données de santé et le service d'accès aux données de santé de l'Union si le pays tiers concerné:

a) est un participant autorisé en raison du fait qu'il dispose d'un point de contact national pour l'utilisation secondaire couvert par un acte d'exécution visé à l'article 75, paragraphe 5; ou

b) permet aux demandeurs de données de santé de l'Union d'accéder aux données de santé électroniques dans ce pays tiers à des conditions qui ne sont pas plus restrictives que celles prévues par le présent règlement et que cet accès est dès lors couvert par un acte d'exécution visé au paragraphe 2 du présent article.

2. La Commission peut, par voie d'actes d'exécution, déterminer qu'un pays tiers satisfait à l'exigence énoncée au paragraphe 1, point b), du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2. La Commission met la liste des actes d'exécution adoptés en vertu du présent paragraphe à la disposition du public.

3. La Commission suit les évolutions dans les pays tiers et les organisations internationales qui pourraient avoir une incidence sur l'application des actes d'exécution adoptés en vertu du paragraphe 2, et elle prévoit un réexamen périodique de l'application du présent article.

Lorsque la Commission estime qu'un pays tiers ne satisfait plus à l'exigence prévue au paragraphe 1, point b), du présent article, elle adopte un acte d'exécution abrogeant l'acte d'exécution visé au paragraphe 2 du présent article concernant ce pays tiers qui bénéficie d'un accès. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

CHAPITRE VI

GOUVERNANCE ET COORDINATION EUROPÉENNES

Article 92

Comité de l'espace européen des données de santé

1. Il est institué un comité de l'espace européen des données de santé (ci-après dénommé «comité de l'EEDS») afin de faciliter la coopération et l'échange d'informations entre les États membres et la Commission. Le comité de l'EEDS est composé de deux représentants par État membre, à savoir un représentant pour l'utilisation primaire et un représentant pour l'utilisation secondaire, désignés par chaque État membre. Chaque État membre dispose d'une voix. Les membres du comité de l'EEDS s'engagent à agir dans l'intérêt public et de manière indépendante.

2. Un représentant de la Commission et l'un des représentants des États membres visés au paragraphe 1 coprésident les réunions du comité de l'EEDS.

3. Les autorités de surveillance du marché visées à l'article 43, le comité européen de la protection des données et le Contrôleur européen de la protection des données, l'Agence européenne des médicaments, le Centre européen de prévention et de contrôle des maladies et l'Agence de l'Union européenne pour la cybersécurité (ENISA) sont invités à assister aux réunions lorsque le comité de l'EEDS l'estime pertinent.

4. Le comité de l'EEDS peut inviter des autorités nationales, des experts et des observateurs ainsi que des institutions, organes et organismes de l'Union, outre ceux visés au paragraphe 3, et des infrastructures de recherche et d'autres infrastructures similaires à assister à ses réunions.

5. Le comité de l'EEDS peut, le cas échéant, coopérer avec des experts externes.

6. Selon les fonctions liées à l'utilisation des données de santé électroniques, le comité de l'EEDS peut travailler en sous-groupes pour certains sujets, dans lesquels les autorités de santé numérique ou les organismes responsables de l'accès aux données de santé sont représentés. Ces sous-groupes soutiennent le comité de l'EEDS en apportant une expertise spécifique et peuvent tenir des réunions conjointes, en tant que de besoin.

7. Le comité de l'EEDS adopte son règlement intérieur et un code de conduite, sur proposition de la Commission. Ce règlement intérieur prévoit la composition, l'organisation, le fonctionnement et la coopération des sous-groupes visés au paragraphe 6 du présent article, ainsi que la coopération du comité de l'EEDS avec le forum des parties prenantes visé à l'article 93.

Le comité de l'EEDS adopte ses décisions par consensus dans la mesure du possible. S'il est impossible de parvenir à un consensus, le comité de l'EEDS adopte ses décisions à la majorité des deux tiers des États membres.

8. Le comité de l'EEDS coopère avec d'autres organismes, entités et experts concernés, tels que le comité européen de l'innovation dans le domaine des données institué par l'article 29 du règlement (UE) 2022/868, les autorités compétentes désignées conformément à l'article 37 du règlement (UE) 2023/2854, les organes de contrôle désignés conformément à l'article 46 *ter* du règlement (UE) n° 910/2014, le comité européen de la protection des données institué par l'article 68 du règlement (UE) 2016/679, les organes de cybersécurité, dont l'ENISA, et le nuage européen pour la science ouverte, en vue de parvenir à des solutions avancées pour l'utilisation de données faciles à trouver, accessibles, interopérables et réutilisables (FAIR) dans la recherche et l'innovation.

9. Le comité de l'EEDS est assisté par un secrétariat assuré par la Commission.

10. Le comité de l'EEDS publie les dates de ses réunions et les comptes rendus de ses débats, ainsi qu'un rapport de ses activités tous les deux ans.

11. La Commission adopte, par voie d'actes d'exécution, les mesures nécessaires à la création et au fonctionnement du comité de l'EEDS. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 93

Forum des parties prenantes

1. Un forum des parties prenantes est institué afin de faciliter l'échange d'informations et de promouvoir la coopération entre les parties prenantes dans le cadre de la mise en œuvre du présent règlement.

2. Le forum des parties prenantes présente une composition équilibrée, est composé des parties prenantes concernées, notamment des représentants des organisations de patients, des professionnels de la santé, des entreprises, des organisations de consommateurs, des chercheurs scientifiques et du monde universitaire, et représente leurs points de vue. Lorsque des intérêts commerciaux sont représentés au sein du forum des parties prenantes, la représentation de ces intérêts est fondée sur une combinaison équilibrée de grandes entreprises, de petites et moyennes entreprises et de start-up. Les tâches du forum des parties prenantes portent de manière égale sur l'utilisation primaire et l'utilisation secondaire.

3. Les membres du forum des parties prenantes sont nommés par la Commission à l'issue d'un appel public à manifestation d'intérêt et d'une procédure de sélection transparente. Les membres du forum des parties prenantes font une déclaration annuelle d'intérêts, qui est rendue publique et mise à jour le cas échéant.

4. Le forum des parties prenantes peut créer des sous-groupes permanents ou temporaires, selon qu'il convient, afin d'examiner des questions spécifiques liées aux objectifs du présent règlement. Le forum des parties prenantes adopte son règlement intérieur.

5. Le forum des parties prenantes se réunit régulièrement et un représentant de la Commission préside les réunions.

6. Le forum des parties prenantes prépare un rapport annuel sur ses activités. Ce rapport est rendu public.

Article 94

Tâches du comité de l'EEDS

1. Le comité de l'EEDS est chargé des tâches ci-après relatives à l'utilisation primaire conformément aux chapitres II et III:

a) aider les États membres à coordonner les pratiques des autorités de santé numérique;

b) fournir des contributions écrites et échanger de bonnes pratiques sur les questions liées à la coordination de la mise en œuvre, à l'échelon des États membres en tenant compte de l'échelon régional et local, du présent règlement et des actes délégués et d'exécution adoptés en vertu de celui-ci, notamment en ce qui concerne:

i) les dispositions des chapitres II et III;

ii) la mise au point de services en ligne facilitant l'accès sécurisé, y compris l'identification électronique sécurisée, aux données de santé électroniques pour les professionnels de la santé et les personnes physiques;

iii) d'autres aspects de l'utilisation primaire;

c) faciliter la coopération entre les autorités de santé numérique par le renforcement des capacités, la mise en place du cadre pour l'élaboration des rapports d'activité visés à l'article 20 et l'échange d'informations;

d) échanger des informations entre ses membres concernant les risques présentés par les systèmes de DME et les incidents graves ainsi que la gestion de ces risques et incidents;

e) faciliter l'échange de vues sur l'utilisation primaire avec le forum des parties prenantes visé à l'article 93, ainsi qu'avec les autorités de réglementation et les décideurs dans le secteur de la santé.

2. Le comité de l'EEDS est chargé des tâches ci-après relatives à l'utilisation secondaire conformément au chapitre IV:

a) aider les États membres à coordonner les pratiques des organismes responsables de l'accès aux données de santé dans la mise en œuvre des dispositions énoncées au chapitre IV, afin d'assurer une application cohérente du présent règlement;

b) fournir des contributions écrites et échanger de bonnes pratiques sur les questions liées à la coordination de la mise en œuvre, à l'échelon des États membres, du présent règlement et des actes délégués et d'exécution adoptés en vertu de celui-ci, notamment en ce qui concerne:

i) la mise en œuvre des règles relatives à l'accès aux données de santé électroniques;

ii) les spécifications techniques ou les normes existantes se rapportant aux exigences énoncées au chapitre IV;

iii) les incitations visant à promouvoir l'amélioration de la qualité des données et de l'interopérabilité;

iv) les politiques relatives aux redevances à percevoir par les organismes responsables de l'accès aux données de santé et les détenteurs de données de santé;

v) les mesures destinées à protéger les données à caractère personnel des professionnels de la santé intervenant dans le traitement de personnes physiques;

vi) d'autres aspects de l'utilisation secondaire;

c) créer, en concertation et en coopération avec les parties prenantes concernées, dont les représentants des patients, des professionnels de la santé et des chercheurs, des lignes directrices afin d'aider les utilisateurs de données de santé à remplir leurs obligations au titre de l'article 61, paragraphe 5, et en particulier en vue de déterminer si leurs constatations sont cliniquement significatives ou non;

d) faciliter la coopération entre les organismes responsables de l'accès aux données de santé par le renforcement des capacités, mettre en place le cadre pour l'élaboration des rapports d'activité visés à l'article 59, paragraphe 1, et l'échange d'informations;

e) échanger des informations concernant les risques et les incidents ayant trait à l'utilisation secondaire et gérer ces risques et incidents;

f) faciliter l'échange de vues sur l'utilisation secondaire avec le forum des parties prenantes visé à l'article 93, ainsi qu'avec les détenteurs de données de santé, les utilisateurs de données de santé, les autorités de réglementation et les décideurs dans le secteur de la santé.

Article 95

Groupes de pilotage pour MaSanté@UE (MyHealth@EU) et DonnéesDeSanté@UE (HealthData@EU)

1. Le groupe de pilotage MaSanté@UE (MyHealth@EU) et le groupe de pilotage DonnéesDeSanté@UE (HealthData@EU) (ci-après dénommés «groupes de pilotage») sont établis pour les infrastructures transfrontières prévues aux articles 23 et 75. Chaque groupe de pilotage est composé d'un représentant par État membre désigné parmi les points de contact nationaux concernés.

2. Les groupes de pilotage prennent des décisions opérationnelles concernant le développement et l'exploitation de MaSanté@UE (MyHealth@EU) et DonnéesDeSanté@UE (HealthData@EU).

3. Les groupes de pilotage prennent leurs décisions par consensus. Lorsqu'il n'est pas possible de parvenir à un consensus, une décision est adoptée à la majorité des deux tiers des membres. Pour l'adoption des décisions, chaque État membre dispose d'une voix.

4. Les groupes de pilotage adoptent un règlement intérieur, fixant la composition, l'organisation, le fonctionnement et la coopération desdits groupes de pilotage.

5. D'autres participants autorisés peuvent être invités à échanger des informations et des points de vue sur des questions pertinentes liées à MaSanté@UE (MyHealth@EU) et DonnéesDeSanté@UE (HealthData@EU). Lorsque ces participants autorisés sont invités, ils ont un rôle d'observateur.

6. Les parties prenantes et les tiers concernés, dont les représentants des patients, des professionnels de la santé, des consommateurs et des entreprises, peuvent être invités à assister aux réunions des groupes de pilotage en qualité d'observateurs.

7. Les groupes de pilotage élisent des présidents pour leurs réunions.

8. Les groupes de pilotage sont assistés par un secrétariat assuré par la Commission.

Article 96

Rôles et responsabilités de la Commission concernant le fonctionnement de l'EEDS

1. Outre son rôle dans la mise à disposition des données de santé électroniques détenues par les institutions, organes ou organismes de l'Union, conformément à l'article 55, à l'article 56 et à l'article 75, paragraphe 2, et les tâches qui lui incombent au titre du chapitre III, en particulier de l'article 40, la Commission développe, maintient, héberge et exploite les infrastructures et les services centraux nécessaires pour soutenir le fonctionnement de l'EEDS, pour toutes les entités connectées concernées, par le biais:

a) d'un mécanisme interopérable et transfrontière d'identification et d'authentification pour les personnes physiques et les professionnels de la santé, conformément à l'article 16, paragraphes 3 et 4;

b) des services centraux et des infrastructures de santé numérique de MaSanté@UE (MyHealth@EU), conformément à l'article 23, paragraphe 1;

c) de contrôles de conformité pour connecter les participants autorisés à MaSanté@UE (MyHealth@EU), conformément à l'article 23, paragraphe 9;

d) des services et infrastructures transfrontières de santé numérique supplémentaires visés à l'article 24, paragraphe 1;

e) dans le cadre de DonnéesDeSanté@UE (HealthData@EU), d'un service auquel présenter des demandes d'accès aux données de santé visant à demander l'accès aux données de santé électroniques détenues par des détenteurs de données de santé dans plus d'un État membre ou par d'autres participants autorisés à DonnéesDeSanté@UE (HealthData@EU), et permettant de transmettre automatiquement les demandes d'accès aux demandes de santé aux points de contact concernés, conformément à l'article 67, paragraphe 3;

f) des services centraux et des infrastructures de DonnéesDeSanté@UE (HealthData@EU), conformément à l'article 75, paragraphes 7 et 8;

g) d'un environnement de traitement sécurisé, conformément à l'article 75, paragraphe 9, dans lequel les organismes responsables de l'accès aux données de santé peuvent décider de mettre des données à disposition, conformément à l'article 68, paragraphe 8;

h) de contrôles de conformité pour connecter les participants autorisés à DonnéesDeSanté@UE (HealthData@EU), conformément à l'article 75, paragraphe 5;

i) d'un catalogue fédéré des ensembles de données de l'UE reliant les catalogues d'ensembles de données nationaux, conformément à l'article 79;

j) d'un secrétariat pour le comité de l'EEDS, conformément à l'article 92, paragraphe 9;

k) d'un secrétariat pour les groupes de pilotage, conformément à l'article 95, paragraphe 8.

2. Les services visés au paragraphe 1 du présent article répondent à des normes de qualité suffisante en matière de disponibilité, de sécurité, de capacité, d'interopérabilité, de maintenance, de suivi et de développement pour garantir le bon fonctionnement de l'EEDS. La Commission fournit ces services conformément aux décisions opérationnelles des groupes de pilotage établis à l'article 95.

3. La Commission prépare un rapport sur les infrastructures et les services qui soutiennent l'EEDS qu'elle fournit conformément au paragraphe 1 tous les deux ans et met ce rapport à la disposition du public.

CHAPITRE VII

DÉLÉGATION DE POUVOIRS ET COMITÉ

Article 97

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 14, paragraphe 2, à l'article 49, paragraphe 4, et à l'article 78, paragraphe 5, est conféré à la Commission pour une durée indéterminée du 25 mars 2025.

3. La délégation de pouvoir visée à l'article 14, paragraphe 2, à l'article 49, paragraphe 4, et à l'article 78, paragraphe 5, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 14, paragraphe 2, de l'article 49, paragraphe 4, ou de l'article 78, paragraphe 5, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 98

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

CHAPITRE VIII

DIVERS

Article 99

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues aux articles 63 et 64, et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 26 mars 2027, du régime ainsi déterminé et des mesures ainsi prises, et lui communiquent sans retard toute modification apportée ultérieurement à ce régime ou à ces mesures.

Les États membres tiennent compte, le cas échéant, des critères indicatifs et non exhaustifs suivants pour l'imposition de sanctions en cas de violation du présent règlement:

a) la nature, la gravité, l'ampleur et la durée de la violation;

b) toute mesure prise par l'auteur de la violation pour atténuer ou réparer le dommage causé par la violation;

c) toute violation antérieure commise par l'auteur de la violation;

d) les avantages financiers obtenus ou les pertes évitées par l'auteur de la violation en raison de la violation, si ces avantages ou pertes peuvent être établis de manière fiable;

e) toute autre circonstance aggravante ou atténuante applicable au cas concerné;

f) le chiffre d'affaires annuel réalisé dans l'Union par l'auteur de la violation au cours de l'exercice précédent.

Article 100

Droit d'obtenir réparation

Toute personne physique ou morale ayant subi un préjudice matériel ou moral résultant de la violation du présent règlement a le droit d'obtenir réparation conformément au droit de l'Union et au droit national.

Article 101

Représentation d'une personne physique

Lorsqu'une personne physique estime que les droits que lui confère le présent règlement ont été violés, elle a le droit de mandater un organisme, une organisation ou une association à but non lucratif, constitués conformément au droit national, dont les objectifs statutaires sont d'intérêt public et qui sont actifs dans le domaine de la protection des données à caractère personnel, pour qu'ils introduisent une réclamation en son nom ou exercent les droits visés aux articles 21 et 81.

Article 102

Évaluation, réexamen et rapport d'avancement

1. Au plus tard le 26 mars 2033, la Commission procède à une évaluation ciblée du présent règlement, et présente au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions un rapport exposant ses principales conclusions, accompagné, s'il y a lieu, d'une proposition de modification. Cette évaluation couvre les éléments suivants:

a) les possibilités d'étendre davantage l'interopérabilité entre les systèmes de DME et les services d'accès aux données de santé électroniques autres que ceux mis en place par les États membres;

b) la nécessité de mettre à jour les catégories de données visées à l'article 51 et les finalités énumérées à l'article 53, paragraphe 1;

c) la mise en œuvre et l'utilisation par les personnes physiques des mécanismes de refus en ce qui concerne l'utilisation secondaire visés à l'article 71, notamment en ce qui concerne l'incidence de ces mécanismes sur la santé publique, la recherche scientifique et les droits fondamentaux;

d) l'utilisation et la mise en œuvre de toutes mesures plus strictes introduites en vertu de l'article 51, paragraphe 4;

e) l'exercice et la mise en œuvre du droit visé à l'article 8;

f) une évaluation du cadre de certification des systèmes de DME établi au chapitre III et la nécessité de mettre en place d'autres outils en matière d'évaluation de la conformité;

g) une évaluation du fonctionnement du marché intérieur pour les systèmes de DME;

h) une évaluation des coûts et des avantages découlant de la mise en œuvre des dispositions relatives à l'utilisation secondaire énoncées au chapitre IV;

i) l'application des redevances visées à l'article 62.

2. Au plus tard le 26 mars 2035, la Commission procède à une évaluation globale du présent règlement, et présente au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions un rapport exposant ses principales conclusions, accompagné, s'il y a lieu, d'une proposition de modification ou d'autres mesures appropriées. Cette évaluation comprend une appréciation de l'efficacité et du fonctionnement des systèmes permettant l'accès aux données de santé électroniques en vue d'un traitement ultérieur, effectué sur la base du droit de l'Union ou du droit national visé à l'article 1er, paragraphe 7, pour ce qui est de leur incidence sur la mise en œuvre du présent règlement.

3. Les États membres fournissent à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 1 et 2, et la Commission tient dûment compte de ces informations dans ces rapports.

4. Chaque année après le 25 mars 2025 et jusqu'à la fin de l'année durant laquelle toutes les dispositions du présent règlement s'appliquent comme prévu à l'article 105, la Commission présente au Conseil un rapport d'avancement sur les préparatifs en vue de la pleine mise en œuvre du présent règlement. Ce rapport d'avancement contient des informations sur le degré d'avancement et de préparation des États membres en ce qui concerne la mise en œuvre du présent règlement, y compris une évaluation de la possibilité de respecter les délais fixés à l'article 105, et peut également contenir des recommandations à l'intention des États membres afin qu'ils soient mieux préparés à l'application du présent règlement.

Article 103

Modification de la directive 2011/24/UE

L'article 14 de la directive 2011/24/UE est supprimé avec effet au 26 mars 2031.

Article 104

Modification du règlement (UE) 2024/2847

Le règlement (UE) 2024/2847 est modifié comme suit:

1) À l'article 13, le paragraphe 4 est remplacé par le texte suivant:

«4. Lorsqu'il met sur le marché un produit comportant des éléments numériques, le fabricant inclut l'évaluation des risques de cybersécurité visée au paragraphe 3 du présent article dans la documentation technique requise conformément à l'article 31 et à l'annexe VII. Pour les produits comportant des éléments numériques mentionnés à l'article 12 et à l'article 32, paragraphe 5 *bis*, qui relèvent aussi d'autres actes juridiques de l'Union, l'évaluation des risques de cybersécurité peut faire partie de l'évaluation des risques prévue par ces actes juridiques de l'Union. Lorsque certaines exigences essentielles en matière de cybersécurité ne sont pas applicables au produit comportant des éléments numériques, le fabricant fait figurer une justification claire dans cette documentation technique.».

2) À l'article 31, le paragraphe 3 est remplacé par le texte suivant:

«3. Pour les produits comportant des éléments numériques visés à l'article 12 et à l'article 32, paragraphe 5 *bis*, qui relèvent aussi d'autres actes juridiques de l'Union prévoyant une documentation technique, une seule documentation technique est établie, contenant les informations visées à l'annexe VII ainsi que les informations requises en vertu de ces actes juridiques de l'Union.».

3) À l'article 32, le paragraphe suivant est inséré:

«5 *bis*. Les fabricants de produits comportant des éléments numériques qui sont classés comme systèmes de DME en vertu du règlement (UE) 2025/327 du Parlement européen et du Conseil (*) démontrent la conformité aux exigences essentielles énoncées à l'annexe I du présent règlement en suivant la procédure d'évaluation de la conformité pertinente prévue au chapitre III du règlement (UE) 2025/327.

(*) Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847 (JO L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj).».

CHAPITRE IX

APPLICATION DIFFÉRÉE, DISPOSITIONS TRANSITOIRES ET DISPOSITIONS FINALES

Article 105

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est applicable à partir du 26 mars 2027.

Cependant, les articles 3 à 15, l'article 23, paragraphes 2 à 6, et les articles 25, 26, 27, 47, 48 et 49 s'appliquent comme suit:

a) à partir du 26 mars 2029 aux catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14, paragraphe 1, points a), b) et c), et aux systèmes de DME destinés par le fabricant à traiter ces catégories de données;

b) à partir du 26 mars 2031 aux catégories prioritaires de données de santé électroniques à caractère personnel visées à l'article 14, paragraphe 1, points d), e) et f), et aux systèmes de DME destinés par le fabricant à traiter ces catégories de données;

c) à partir d'un an à compter de la date fixée dans un acte délégué à adopter en vertu de l'article 14, paragraphe 2, pour chaque modification des principales caractéristiques des données de santé électroniques à caractère personnel figurant à l'annexe I, à condition que cette date soit postérieure à la date d'application visée aux points a) et b) du présent alinéa pour les catégories de données de santé électroniques à caractère personnel concernées.

Le chapitre III s'applique aux systèmes de DME mis en service dans l'Union visés à l'article 26, paragraphe 2, à partir du 26 mars 2031.

Le chapitre IV s'applique à partir du 26 mars 2029. Cependant, l'article 55, paragraphe 6, l'article 70, l'article 73, paragraphe 5, l'article 75, paragraphes 1 et 12, l'article 77, paragraphe 4, et l'article 78, paragraphe 6, s'appliquent à partir du 26 mars 2027. L'article 51, paragraphe 1, points b), f), g), m) et p), s'applique à partir du 26 mars 2031, et l'article 75, paragraphe 5, s'applique à partir du 26 mars 2035.

Les actes d'exécution visés à l'article 13, paragraphe 4, à l'article 15, paragraphe 1, à l'article 23, paragraphe 4, et à l'article 36, paragraphe 1, s'appliquent à partir des dates visées au troisième alinéa du présent article en fonction des catégories de données de santé électroniques à caractère personnel visées à l'article 14, paragraphe 1, points a), b) et c), ou à l'article 14, paragraphe 1, points d), e) et f), respectivement.

Les actes d'exécution visés à l'article 70, à l'article 73, paragraphe 5, à l'article 75, paragraphe 12, à l'article 77, paragraphe 4, et à l'article 78, paragraphe 6, s'appliquent à partir du 26 mars 2029.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 11 février 2025.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	A. SZŁAPKA

ANNEXE I

Principales caractéristiques des catégories prioritaires de données de santé électroniques à caractère personnel à des fins d'utilisation primaire

Catégorie de données de santé électroniques	Principales caractéristiques des données de santé électroniques incluses dans la catégorie
1. Résumés des dossiers de patients	Données de santé électroniques qui incluent des faits cliniques importants concernant une personne physique identifiée et qui sont essentielles à la fourniture sûre et efficiente de soins de santé à cette personne. Les informations suivantes font partie d'un résumé du dossier de patient: 1. Données d'identification personnelle. 2. Coordonnées. 3. Informations relatives aux assurances. 4. Allergies. 5. Alertes médicales. 6. Informations de vaccination/prophylaxie, éventuellement sous la forme d'un carnet de vaccination. 7. Problèmes actuels, résolus, clos ou inactifs, y compris dans un système international de codage avec classification. 8. Informations textuelles relatives aux antécédents médicaux. 9. Dispositifs médicaux et implants. 10. Procédures médicales ou de soins. 11. État fonctionnel. 12. Médicaments actuels et passés pertinents. 13. Observations concernant les antécédents sociaux relatives à la santé. 14. Antécédents de grossesse. 15. Données fournies par le patient. 16. Résultats d'observation concernant l'état de santé. 17. Plan de soins. 18. Informations relatives à une maladie rare, telles que les détails de l'incidence ou des caractéristiques de la maladie.
2. Prescriptions électroniques	Données de santé électroniques constituant une prescription pour un médicament tel qu'il est défini à l'article 3, point k), de la directive 2011/24/UE.
3. Dispensations électroniques	Informations relatives à la fourniture d'un médicament à une personne physique par une pharmacie sur la base d'une prescription électronique.
4. Examens d'imagerie médicale et comptes rendus d'imagerie médicale y afférents	Données de santé électroniques relatives à l'utilisation de technologies qui sont utilisées pour visualiser le corps humain afin de prévenir, diagnostiquer, surveiller ou traiter des problèmes médicaux, ou produites par ces technologies.
5. Résultats d'examens médicaux, y compris les résultats de laboratoire et d'autres diagnostics, ainsi que les comptes rendus y afférents	Données de santé électroniques représentant les résultats d'études réalisées notamment au moyen de techniques de diagnostic in vitro comme la biochimie clinique, l'hématologie, la médecine transfusionnelle, la microbiologie, l'immunologie et d'autres, et y compris, le cas échéant, les rapports corroborant l'interprétation des résultats.
6. Rapports de sortie d'hôpital	Données de santé électroniques relatives à une visite médicale ou à un épisode de soins et comprenant des informations essentielles sur l'admission, le traitement et la sortie d'une personne physique.

ANNEXE II

Exigences essentielles applicables aux composants logiciels harmonisés des systèmes de DME et aux produits pour lesquels l'interopérabilité avec les systèmes de DME est alléguée

Les exigences essentielles définies dans la présente annexe s'appliquent mutatis mutandis aux dispositifs médicaux, aux dispositifs médicaux de diagnostic in vitro, aux systèmes d'IA et aux applications de bien-être au sujet desquelles l'interopérabilité avec les systèmes de DME est alléguée.

1. Exigences générales

1.1. Les composants logiciels harmonisés d'un système de DME doivent atteindre le niveau de performance prévu par son fabricant et être conçus et fabriqués de manière à être adaptés à leur destination et que leur utilisation ne mette pas en péril la sécurité des patients dans des conditions normales d'utilisation.

1.2. Les composants logiciels harmonisés du système de DME doivent être conçus et élaborés de manière que le système de DME puisse être livré et installé, en tenant compte des instructions et des informations fournies par le fabricant, sans qu'il n'y ait d'effets négatifs sur ses caractéristiques et ses performances au cours de l'utilisation prévue.

1.3. Un système de DME doit être conçu et élaboré de manière que ses dispositifs d'interopérabilité, de sûreté et de sécurité protègent les droits des personnes physiques, conformément à la destination du système de DME, comme établi au chapitre II.

1.4. Les composants logiciels harmonisés d'un système de DME destiné à fonctionner en combinaison avec d'autres produits, notamment des dispositifs médicaux, doivent être conçus et fabriqués de manière que l'interopérabilité et la compatibilité soient fiables et sûres, et à ce que les données de santé électroniques à caractère personnel puissent être partagées entre le dispositif et le système de DME en ce qui concerne ces composants logiciels harmonisés d'un système de DME.

2. Exigences en matière d'interopérabilité

2.1. Lorsqu'un système de DME est conçu pour stocker des données de santé électroniques à caractère personnel ou faire office d'intermédiaire pour ces données, il fournit une interface permettant d'accéder aux données de santé électroniques à caractère personnel qu'il traite dans le format européen d'échange des dossiers médicaux électroniques, au moyen du composant logiciel d'interopérabilité européen pour les systèmes de DME.

2.2. Lorsqu'un système de DME est conçu pour stocker des données de santé électroniques à caractère personnel ou faire office d'intermédiaire pour ces données, il est en mesure de recevoir des données de santé électroniques à caractère personnel dans le format européen d'échange des dossiers médicaux électroniques, au moyen du composant logiciel d'interopérabilité européen pour les systèmes de DME.

2.3. Lorsqu'un système de DME est conçu pour donner accès à des données de santé électroniques à caractère personnel, il est en mesure de recevoir des données de santé électroniques à caractère personnel dans le format européen d'échange des dossiers médicaux électroniques, au moyen du composant logiciel d'interopérabilité européen pour les systèmes de DME.

2.4. Un système de DME qui comporte une fonctionnalité permettant d'introduire des données de santé électroniques à caractère personnel structurées doit permettre l'introduction de ces données avec une granularité suffisante pour permettre de fournir les données de santé électroniques à caractère personnel introduites dans le format européen d'échange des dossiers médicaux électroniques.

2.5. Les composants logiciels harmonisés d'un système de DME ne doivent pas comporter de fonctionnalité qui interdise ou restreigne l'accès autorisé, le partage de données de santé électroniques à caractère personnel, ou l'utilisation de données de santé électroniques à caractère personnel à des fins autorisées, ou qui impose des contraintes excessives à cet égard.

2.6. Les composants logiciels harmonisés d'un système de DME ne doivent pas comporter de fonctionnalité qui interdise ou restreigne l'exportation autorisée de données de santé électroniques à caractère personnel aux fins de remplacer le système de DME par un autre produit, ou qui impose des contraintes excessives à cet égard.

3. Exigences en matière de sécurité et de journalisation

3.1. Un système de DME destiné à être utilisé par les professionnels de la santé doit prévoir des mécanismes fiables d'identification et d'authentification des professionnels de la santé.

3.2. Le composant logiciel de journalisation européen d'un système de DME destiné à permettre l'accès des prestataires de soins de santé ou d'autres personnes aux données de santé électroniques à caractère personnel doit prévoir des mécanismes de journalisation suffisants qui enregistrent, au minimum, les informations suivantes lors de chaque événement d'accès ou groupe d'événements:

a) l'identification du prestataire de soins de santé ou de toute autre personne ayant accédé aux données de santé électroniques à caractère personnel;

b) l'identification de la ou des personnes physiques spécifiques ayant accédé aux données de santé électroniques à caractère personnel;

c) les catégories de données consultées;

d) l'heure et la date de l'accès;

e) l'origine ou les origines des données.

3.3. Les composants logiciels harmonisés d'un système de DME doivent comporter des outils ou des mécanismes visant à passer en revue et à analyser les données du journal, ou doivent permettre la connexion à un logiciel externe, ou l'utilisation de celui-ci, à ces mêmes fins.

3.4. Les composants logiciels harmonisés d'un système de DME qui stockent des données de santé électroniques à caractère personnel doivent permettre différentes périodes de rétention et droits d'accès qui tiennent compte des origines et des catégories des données de santé électroniques.

ANNEXE III

Documentation technique

La documentation technique visée à l'article 37 contient au moins les informations ci-après, selon qu'elles s'appliquent aux composants logiciels harmonisés d'un système de DME dans le système de DME concerné:

1) une description détaillée du système de DME, notamment:
   a) sa destination, ainsi que la date et la version du système de DME;
   b) les catégories de données de santé électroniques à caractère personnel pour le traitement desquelles le système de DME a été conçu;
   c) la manière dont le système de DME interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels qui ne font pas partie du système de DME lui-même;
   d) les versions des logiciels ou des micrologiciels pertinents et toute exigence relative à la mise à jour de la version;
   e) la description de toutes les formes sous lesquelles le système de DME est mis sur le marché ou mis en service;
   f) la description du matériel informatique sur lequel le système de DME est destiné à être exécuté;
   g) une description de l'architecture du système expliquant comment les composants logiciels s'appuient les uns sur les autres ou s'alimentent les uns les autres et s'intègrent dans le traitement global, y compris, le cas échéant, des représentations graphiques étiquetées (par exemple, des diagrammes et des dessins), indiquant clairement les éléments ou composants logiciels clés et incluant une explication suffisante pour comprendre les dessins et les diagrammes;
   h) les spécifications techniques, telles que les fonctionnalités, dimensions et caractéristiques de performance, du système de DME et de toute variante ou configuration ou de tout accessoire qui figurent habituellement dans les spécifications du produit mises à disposition de l'utilisateur, par exemple dans des brochures, des catalogues et des publications similaires, y compris une description détaillée des structures de données, du stockage et des entrées/sorties de données;
   i) une description des éventuelles modifications apportées au système tout au long de son cycle de vie;
   j) la notice d'utilisation pour l'utilisateur et, le cas échéant, des instructions d'installation;
2) une description détaillée du système en place pour évaluer les performances du système de DME, le cas échéant;
3) les références aux spécifications communes qui ont été utilisées conformément à l'article 36 et par rapport auxquelles la conformité est déclarée;
4) les résultats et les analyses critiques de toutes les vérifications et de tous les essais de validation réalisés pour démontrer la conformité du système de DME avec les exigences définies au chapitre III, en particulier les exigences essentielles applicables;
5) une copie de la fiche d'information visée à l'article 38;
6) une copie de la déclaration UE de conformité.

ANNEXE IV

Déclaration UE de conformité

La déclaration UE de conformité pour les composants logiciels harmonisés d'un système de DME contient l'ensemble des informations suivantes:

1) le nom du système de DME, la version et toute référence sans équivoque supplémentaire permettant d'identifier le système de DME;

2) le nom et l'adresse du fabricant ou, le cas échéant, de son mandataire;

3) une déclaration attestant que la déclaration UE de conformité est délivrée sous la seule responsabilité du fabricant;

4) une déclaration attestant que le système de DME en question respecte les dispositions établies au chapitre III et, le cas échéant, toute autre disposition du droit de l'Union applicable prévoyant la délivrance d'une déclaration UE de conformité, complétée par les résultats de l'environnement d'essai mentionné à l'article 40;

5) des références aux normes harmonisées pertinentes qui ont été utilisées et par rapport auxquelles la conformité est déclarée;

6) des références aux spécifications communes qui ont été utilisées et par rapport auxquelles la conformité est déclarée;

7) le lieu et la date de délivrance de la déclaration, la signature, le nom et la fonction du signataire et, le cas échéant, une indication de la personne au nom de laquelle elle a été signée;

8) le cas échéant, des informations supplémentaires.