Groupe de travail «ARTICLE 29» sur la protection des données

00323/07/FR
WP 131

Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)

Adopté le 15 février 2007

S Y N T H È S E

Dans le présent document de travail sur le **traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)**, le groupe de travail «Article 29» donne des indications au sujet de l'interprétation du cadre juridique de protection des données applicable aux systèmes de DME et explique certains principes généraux. Il donne également des indications au sujet des exigences en matière de protection des données auxquelles doit satisfaire l'institution de systèmes de DME ainsi que les garanties applicables.

Le groupe de travail «Article 29» examine d'abord le **cadre juridique général de protection des données** pour les systèmes de DME. Il rappelle l'interdiction générale du traitement de données à caractère personnel relatives à la santé énoncée à l'article 8, paragraphe 1, de la directive 95/46/CE sur la protection des données et examine ensuite l'éventuelle application des dérogations prévues à l'article 8, paragraphes 2, 3 et 4, de cette même directive dans le cadre des systèmes de DME en insistant sur la nécessité d'une interprétation stricte de ces dérogations.

Le groupe de travail «Article 29» réfléchit également à un **cadre juridique adapté aux systèmes de DME** et formule des **recommandations sur onze sujets** pour lesquels des garanties spéciales au sein des systèmes de DME semblent particulièrement nécessaires afin de garantir les droits à la protection des données des patients et des personnes. Il s'agit des sujets suivants:

1. le respect de l'autodétermination;
2. l'identification et l'authentification des patients et des professionnels de santé;
3. l'autorisation d'accéder aux DME pour lecture et écriture;
4. l'utilisation des DME à d'autres fins;
5. la structure organisationnelle d'un système de DME;
6. les catégories de données stockées dans les DME et leurs modes de présentation;
7. le transfert international des dossiers médicaux;
8. la sécurité des données;
9. la transparence;
10. les questions de responsabilité;
11. les mécanismes de contrôle du traitement des données contenues dans les DME.

Le groupe de travail «Article 29» invite le corps médical, tous les professionnels de santé, toutes les personnes et les institutions concernées et la population en général à formuler des commentaires sur le présent document de travail.

TABLE DES MATIERES

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1], notamment ses articles 29 et 30, paragraphe 1, point b),

vu le règlement intérieur du groupe de travail[2], notamment ses articles 12 et 14,

A ADOPTÉ LE DOCUMENT DE TRAVAIL SUIVANT:

I. Introduction

L'objectif du présent document de travail du groupe de travail «Article 29» est de donner des indications au sujet de l'interprétation du cadre juridique de protection des données applicable aux systèmes de dossier médical électronique (DME) et d'énoncer certains principes généraux. Il vise également à définir les conditions de protection des données nécessaires à l'institution d'un système de DME à l'échelle nationale ainsi que les garanties applicables.

Les coûts des systèmes publics de soins de santé augmentent de façon spectaculaire et les gouvernements réclament de nouvelles stratégies pour faire face à ce problème. L'une des réponses souvent proposées est le «dossier médical électronique (DME)». «Dossier de santé électronique (DSE)», «dossier patient électronique (DPE)», «dossier médical électronique (DME)», «dossier patient informatisé (DPI)», etc. sont autant de termes interchangeables utilisés dans ce domaine.

Aux fins du présent document de travail, le «dossier médical électronique (ci-après, DME)» est défini comme suit:

> *«dossier médical complet ou documentation similaire sur l'état de santé physique et mental passé et présent d'une personne sous forme électronique permettant d'accéder facilement à ces données en vue d'un traitement médical et à d'autres fins étroitement liées*[3]*.»*

Auparavant, les documents relatifs aux traitements médicaux étaient disponibles auprès de différents professionnels de santé mais n'étaient pas regroupés en un seul dossier. Le concept de «DME» vise quant à lui à rassembler, à partir de différentes sources et de différentes périodes, les documents existants sur les traitements médicaux d'une même personne. Il donnerait ainsi des informations sur l'état de santé passé et présent d'une personne de la façon

---

1 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données; JO L 281 du 23.11.1995, p. 31 (ci-après, «la directive»); disponible à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/law/index_fr.htm.

2 Adopté par le groupe de travail lors de sa troisième réunion, le 11 septembre 1996.

3 L'expression «un traitement médical et à d'autres fins étroitement liées» renvoie aux finalités mentionnées à l'article 8, paragraphe 3, de la directive.

la plus complète possible, et sur une longue période, peut-être même la vie entière *(«du berceau à la tombe»*). Une fois réunies, les données des DME seraient accessibles sous forme électronique à tous les professionnels de santé habilités et à d'autres institutions autorisées, partout et chaque fois que ces informations sont nécessaires.

Le DME est présenté comme un moyen approprié:

- d'accroître la qualité des traitements grâce à de meilleures informations sur le patient;
- d'améliorer le rapport coût-efficacité des traitements médicaux et d'enrayer ainsi l'augmentation rapide des déficits du budget de la santé;
- de fournir les données nécessaires au contrôle de qualité, aux statistiques et à la planification dans le secteur public des soins de santé, ce qui devrait également avoir des retombées positives sur les budgets publics de santé.

Les réponses à un questionnaire soumis en 2005 aux autorités européennes de contrôle de la protection des données ont montré que les systèmes de DME nationaux sont des sujets pertinents et urgents dans la plupart des États membres. Le degré de réalisation de ces projets est cependant très variable: alors que la plupart des États membres débattent des DME, d'autres ont déjà mis des systèmes de DME en œuvre, du moins en partie.

Les soins de santé étant de plus en plus dispensés au-delà des frontières, la Commission européenne a souligné dans sa communication *«Santé en ligne - Améliorer les soins de santé pour les citoyens européens: plan d'action pour un espace européen de la santé en ligne»*[4], l'importance des services de santé en ligne et de l'interopérabilité des dossiers médicaux électroniques. En outre, la Communauté européenne finance des projets pertinents, relatifs notamment aux dossiers patient électroniques ou aux identifiants des patients (par exemple, la carte européenne d'assurance maladie). Lors de la mise en œuvre de tels programmes, la Commission européenne, en collaboration avec les États membres, doit veiller au respect de toutes les dispositions légales applicables dans le domaine de la protection des données à caractère personnel et, le cas échéant, à l'instauration de mécanismes assurant la confidentialité et la sécurité de ces données[5].

Les systèmes de DME ont le potentiel d'améliorer la qualité et la sécurité des informations médicales par rapport aux formes traditionnelles de documentation médicale. Toutefois, du point de vue de la protection des données, il convient de souligner que les systèmes de DME ont en outre la capacité non seulement de traiter davantage de données à caractère personnel (par exemple dans de nouveaux contextes, ou par agrégation), mais aussi de permettre à un plus grand nombre de destinataires d'accéder plus facilement qu'auparavant aux données d'un patient.

Il faut également noter que les informations électroniques relatives à la santé contenues dans un système de DME – outre qu'elles sont accessibles aux professionnels de santé – pourraient généralement susciter l'intérêt de tiers tels que les compagnies d'assurance et les autorités répressives. Du point de vue de la protection des données à caractère personnel, en rassemblant les informations médicales relatives à une personne en provenance de différentes sources, facilitant et généralisant ainsi l'accès à ces informations sensibles, les systèmes de DME créent de nouveaux risques et donnent une ampleur inédite au danger d'abus des

[4] COM (2004) 356 final.

[5] Voir, par exemple, l'article 5, paragraphe 5, de la décision 1786/2002/CE.

informations médicales relatives aux personnes. Si la plupart des projets ne poseront véritablement ces nouveaux risques que lorsqu'ils seront pleinement mis en œuvre, il faut néanmoins être conscients de ces dangers dès à présent, à un stade où la plupart des modèles existants ne prévoient qu'une application limitée ou partielle (ne concernant, par exemple, qu'une série fondamentale de données médicales ou que les hôpitaux d'une région donnée), puisque ce n'est qu'une question de temps avant qu'ils ne deviennent généralement applicables.

II. Le cadre de protection des données applicable aux dossiers médicaux électroniques

Tout traitement de données à caractère personnel dans les systèmes de DME doit respecter pleinement les règles de protection des données à caractère personnel. Le groupe de travail tient à souligner que le cadre s'appliquant à l'utilisation des DME est exposé au considérant 2 de la directive, selon lequel: *«les systèmes de traitement de données sont au service de l'homme; […] ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus».*

Le droit fondamental à la protection des données à caractère personnel repose essentiellement sur l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et sur l'article 8 de la charte européenne des droits fondamentaux[6]. Des règles plus précises sont notamment définies dans la directive 95/46/CE sur la protection des données et dans la directive 2002/58/CE sur la vie privée et les communications électroniques[7], ainsi que dans les législations nationales des États membres mettant en œuvre ces directives.

Tout traitement de données à caractère personnel contenues dans les DME doit également respecter les règles établies dans la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et dans le protocole additionnel à la convention 108 concernant les autorités de contrôle et les flux transfrontaliers de données (STE n° 181) du Conseil de l'Europe.

Dans le cadre des DME, le groupe de travail tient à attirer particulièrement l'attention sur la recommandation n° R(97) 5 du Conseil de l'Europe sur la protection des données médicales (13 février 1997). Il renvoie également aux recommandations formulées dans le «Working Document on Online Availability of Electronic Health Records» (document de travail sur la

---

6 Le droit à la protection des données à caractère personnel n'est pas absolu et peut être restreint si des intérêts publics spécifiques le requièrent. Cependant, ces objectifs d'intérêt public ne peuvent justifier une atteinte à la protection des données à caractère personnel que si elle est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui et qu'elle n'est pas disproportionnée par rapport à l'objectif poursuivi (article 8, paragraphe 2, de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales).

7 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 (JO L 201 du 31.7.2002, p. 37 à 47).

disponibilité en ligne des dossiers médicaux électroniques) du groupe de travail international sur la protection des données dans les télécommunications[8].

1. Principes généraux

Les responsables du traitement des données qui collectent des données dans le cadre d'applications DME doivent donc respecter tous les principes généraux de protection des données, dont les suivants:

- l'application du principe de limitation (principe des finalités): ce principe, partiellement formulé à l'article 6, paragraphe 1, point b), de la directive, interdit notamment le traitement ultérieur incompatible avec la (les) finalité(s) de la collecte;

- le principe de la qualité des données: ce principe inscrit dans la directive exige que les données à caractère personnel soient pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. Aucune donnée non pertinente ne doit donc être collectée. En cas de collecte de données non pertinentes, elles doivent être supprimées (article 6, paragraphe 1, point c)). Ce principe exige également que les données soient exactes et mises à jour;

- le principe de rétention: ce principe exige que les données à caractère personnel ne soient pas conservées plus longtemps que nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou traitées ultérieurement;

- les exigences en matière d'information: selon l'article 10 de la directive, les responsables du traitement des informations dans les systèmes de DME doivent donner certaines informations aux personnes concernées, notamment sur l'identité du responsable du traitement, sur les finalités du traitement, sur les destinataires des données et sur l'existence d'un droit d'accès;

- le droit d'accès de la personne concernée: l'article 12 de la directive habilite les personnes concernées à vérifier l'exactitude des données et à veiller à leur mise à jour. Ces droits s'appliquent pleinement à la collecte de données à caractère personnel dans les systèmes de DME;

- les obligations relatives à la sécurité: l'article 17 de la directive impose aux responsables du traitement l'obligation de mettre en œuvre les mesures requises pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite ou la diffusion non autorisée. Ces mesures peuvent être techniques ou d'organisation.

2. Protection spéciale pour les données à caractère personnel sensibles

Lorsque le traitement des données à caractère personnel concerne la santé d'une personne, il est particulièrement sensible et requiert dès lors une protection spéciale.

L'article 2, point a), de la directive 95/46/CE définit les données à caractère personnel comme suit:

«"données à caractère personnel": toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une

[8] Adopté lors de sa 39e réunion à Washington D.C., les 6 et 7 avril 2006 (http://www.berlin-privacy-group.org).

personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.»

La définition des catégories spéciales de données contenue à l'article 8, paragraphe 1, de la directive est la suivante:

«Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.»

L'indication du fait qu'une personne s'est blessée au pied et est à temps partiel pour raisons médicales constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive[9]. Cette définition s'applique également aux données à caractère personnel lorsqu'elles présentent un lien clair et étroit avec la description de l'état de santé d'une personne: les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques sont incontestablement des «données à caractère personnel relatives à la santé», en particulier si elles sont consignées dans un dossier médical. En outre, toutes autres données – par exemple des données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.) – contenues dans les documents médicaux relatifs au traitement d'un patient doivent être considérées comme sensibles: si elle n'étaient pas pertinentes dans le cadre du traitement du patient, elles n'auraient pas été, et n'auraient pas dû être, incluses dans un dossier médical.

Les membres du groupe de travail sont par conséquent d'avis que toutes les données contenues dans les documents médicaux, les dossiers médicaux électroniques et les systèmes de DME sont à considérer comme des «données à caractère personnel sensibles». Elles sont donc soumises non seulement à toutes les règles générales sur la protection des données à caractère personnel énoncées dans la directive, mais aussi aux règles spéciales en matière de protection des données relatives au traitement des informations sensibles contenues à l'article 8 de la directive.

3. Une interdiction générale du traitement des données à caractère personnel relatives à la santé –assortie de dérogations

L'article 8, paragraphe 1, de la directive 95/46/CE sur la protection des données interdit à titre général le traitement des données à caractère personnel relatives à la santé. Il en va de même de l'article 6 de la convention n° 108 du Conseil de l'Europe.

Cette protection spéciale prévue à l'article 8, paragraphe 1, complète les autres dispositions de la directive, notamment l'article 6 sur les principes relatifs à la qualité des données et l'article 7 sur les critères à remplir pour légitimer le traitement des données.

Comme il est important d'utiliser les informations relatives à un patient pour lui administrer le traitement médical le plus indiqué, il existe cependant des dérogations à l'interdiction générale du traitement des données médicales.

[9] Cour de justice des Communautés européennes, arrêt du 6 novembre 2003 dans l'affaire C-101/01 – Bodil Lindqvist.

La directive sur la protection des données prévoit des **dérogations obligatoires** à l'article 8, paragraphes 2 et 3, ainsi qu'une **exemption facultative** à l'article 8, paragraphe 4.

Toutes ces dérogations sont **limitées**, **exhaustives** et doivent être **interprétées strictement**.

4. L'article 8, paragraphe 2, point a): le «consentement explicite»

Selon l'article 8, paragraphe 2, point a), de la directive:

> *«Le paragraphe 1 ne s'applique pas lorsque: a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée.»*

a) Le **consentement** de la personne concernée peut donc justifier le traitement de données sensibles[10]. Comme déjà indiqué dans les précédents documents de travail du groupe de travail WP 12[11] et WP 114[12], ce consentement doit, pour être valable, quelles que soient les circonstances dans lesquelles il est donné, être une «*manifestation de volonté, libre, spécifique et informée*», selon la définition qu'en donne l'article 2, point h), de la directive.

> aa) Le consentement doit être donné librement: le consentement «libre» désigne une décision volontaire, prise par une personne en pleine possession de ses facultés, en l'absence de toute coercition, qu'elle soit sociale, financière, psychologique ou autre. Un consentement donné sous la menace de privation de traitement ou de traitement de moindre qualité dans une situation médicale ne saurait être considéré comme «libre». Un consentement donné par une personne qui n'a pas eu la possibilité de faire un véritable choix ou qui a été mise devant le fait accompli ne peut être considéré comme valable.
>
> Le groupe de travail «Article 29» est d'avis que lorsque la situation médicale exige nécessairement et inévitablement que le praticien de santé traite des données à caractère personnel dans un système de DME, il est trompeur que ce praticien cherche à légitimer ce traitement par le consentement. Le recours au consentement doit être limité aux cas où la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice[13].
>
> bb) Le consentement doit être spécifique: le consentement «spécifique» doit porter sur une situation concrète et bien définie, dans laquelle le traitement de données médicales est envisagé. Un «accord global» de la personne concernée, par exemple pour la collecte de ses données médicales pour un DME et pour le transfert ultérieur de ces données médicales passées et futures aux praticiens de santé intervenant dans le traitement n'est donc pas un consentement au sens de l'article 2, paragraphe 2, point h), de la directive.

---

[10] L'acceptation de suivre un traitement médical donné ne constitue pas automatiquement un «consentement» au sens de l'article 2, point h), au traitement (en particulier la communication ou le transfert) des données à caractère personnel collectées durant ce traitement.

[11] «Document de travail: Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» du groupe de travail «Article 29» (WP 12, 24 juillet 1998).

[12] «Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995» du groupe de travail «Article 29» (WP 114, 25 novembre 2005).

[13] Voir également l'«Avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel» du groupe de travail «Article 29» (WP 48, point 10).

cc) Le consentement doit être «informé»: un consentement «informé» signifie qu'il doit être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action. La personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents, en particulier ceux spécifiés aux articles 10 et 11 de la directive, tels que la nature des données traitées, les finalités du traitement, les destinataires d'éventuels transferts et ses droits. Cela suppose également la connaissance des conséquences du refus de consentir au traitement des données en question.

b) Contrairement aux dispositions de l'article 7 de la directive, le consentement dans le cas de données à caractère personnel sensibles, et donc d'un DME, doit être **explicite**. Les solutions qui prévoient un droit de refus ne remplissent pas le critère du caractère «explicite». Conformément à la définition générale selon laquelle le consentement suppose une manifestation de volonté, le caractère explicite doit porter en particulier sur la **nature sensible des données**. La personne concernée doit avoir conscience du fait qu'elle renonce à une protection particulière. Le consentement écrit n'est toutefois pas requis.

c) Le groupe de travail «Article 29» a constaté que le consentement était parfois difficile à obtenir en raison de problèmes pratiques, notamment en l'absence de contact direct entre le responsable du traitement et les personnes concernées. Quelles que puissent être ces difficultés, le **responsable du traitement** doit pouvoir prouver en toutes circonstances, d'une part, qu'il a obtenu le consentement explicite de chaque personne concernée et, d'autre part, que ce consentement a été donné sur la base d'informations suffisamment précises.

d) Contrairement à l'article 7 également, l'article 8, paragraphe 2, point a), reconnaît qu'il peut y avoir des cas de traitement de données sensibles dans lesquels **même le consentement explicite** de la personne concernée ne peut lever l'interdiction du traitement des données: les États membres sont libres de réglementer ces cas et d'en définir les modalités.

5. L'article 8, paragraphe 2, point c): les «intérêts vitaux de la personne concernée»

Le traitement de données à caractère personnel sensibles peut être justifié s'il est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement.

Le traitement des données doit concerner des intérêts personnels essentiels de la personne concernée ou d'une autre personne et doit - dans le contexte médical - être nécessaire à un traitement dont dépend la vie dans une situation où la personne concernée n'est pas en mesure de manifester sa volonté. Par conséquent, cette dérogation ne peut s'appliquer qu'à un nombre limité de traitements médicaux et ne peut en aucun cas être utilisée pour justifier le traitement de données médicales à caractère personnel à d'autres fins que les soins à dispenser à la personne concernée: par exemple, pour mener des recherches médicales générales qui ne donneront pas de résultats avant un certain temps[14].

À titre d'exemple: supposons qu'une personne ait perdu connaissance à la suite d'un accident et ne puisse donner son consentement à la nécessaire divulgation de ses allergies

[14] Pour une interprétation de la disposition similaire de l'article 26, paragraphe 1, point e), en ce qui concerne les transferts de données en dehors de l'UE, voir le «Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995» du groupe de travail «Article 29», WP 114 (25 novembre 2005).

connues. Dans le cadre de systèmes de DME, cette disposition permettrait à un praticien de santé d'accéder aux informations stockées dans le DME afin d'en extraire les informations sur les allergies connues de la personne concernée, car celles-ci pourraient s'avérer déterminantes pour le choix du traitement.

6. L'article 8, paragraphe 3: le «traitement des données (médicales) par un praticien de santé»

L'article 8, paragraphe 3, autorise le traitement de données à caractère personnel sensibles sous trois conditions cumulatives: il doit être *«nécessaire»* et être réalisé *«aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé»* et *[…]* être «*effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente»*.

a) Cette dérogation couvre uniquement le traitement de données à caractère personnel dans le **but spécifique** de fournir des services de santé à caractère préventif, diagnostique, thérapeutique ou de postcure et de gérer ces services de soins de santé, par exemple pour la facturation, la comptabilité ou les statistiques.

Elle ne couvre pas un traitement ultérieur non nécessaire à la fourniture directe de ces services, notamment l'utilisation des données pour la recherche médicale, le remboursement ultérieur des frais par un régime d'assurance maladie ou le recouvrement de créances. Échappent également au champ d'application de l'article 8, paragraphe 3, d'autres opérations de traitement de données dans des domaines tels que la santé publique et la protection sociale, visant notamment à assurer la qualité et la rentabilité des procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie, puisque ces opérations sont mentionnées au considérant 34 de la directive en tant qu'exemples d'invocation de l'article 8, paragraphe 4.

b) De plus, le traitement de données à caractère personnel en vertu de l'article 8, paragraphe 3, doit être **«nécessaire»** aux fins spécifiques mentionnées au point a). Le groupe de travail souligne que, dans le cadre des DME, cela signifie que toute inscription de données à caractère personnel dans un DME doit être pleinement justifiée; la simple «utilité» d'inclure ces données à caractère personnel dans un DME ne suffit pas.

c) La troisième condition de l'article 8, paragraphe 3, est que les données à caractère personnel sensibles soient traitées par un personnel médical ou autre soumis au **secret professionnel (médical) ou à une obligation de secret équivalente**.

> L'exigence éthique de confidentialité imposée au corps médical a été énoncée pour la première fois dans le «serment d'Hippocrate»[15] et a ensuite été confirmée par la déclaration de Genève (1948) de l'Association médicale mondiale. Elle protège les informations recueillies par un professionnel de santé au cours du traitement d'un patient. L'utilisation de ces informations n'est autorisée que dans les limites du contrat de traitement. Cette relation de confidentialité exclut tous les tiers, même les autres professionnels de santé, sauf si le patient a consenti à la transmission des données ou si celle-ci est spécifiquement prévue par la loi.

[15] *«Quoi que je voie ou entende dans la société pendant, ou même hors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas.»* (Source: http://fr.wikipedia.org/wiki/Serment_d%27Hippocrate).

Le groupe de travail signale que l'obligation spécifique de secret professionnel doit être prévue soit dans la législation nationale des États membres, soit par les organismes professionnels nationaux compétents pour adopter des règles contraignantes pour la profession. Ces règles nationales sur le secret professionnel doivent aussi prévoir des sanctions effectives correspondantes en cas de violation.

D'après la directive, s'il s'avérait nécessaire que du personnel non médical traite ces données à caractère personnel sensibles, ce personnel doit également être soumis à des règles contraignantes qui garantissent un niveau au moins équivalent de confidentialité et de protection, et qui prévoient notamment l'obligation de n'utiliser les données qu'aux fins mentionnées à l'article 8, paragraphe 3.

Les praticiens de santé directement responsables du traitement des patients ont généralement l'obligation légale de conserver une documentation sur le traitement médical (actes, prescriptions, etc.) dans les dossiers des patients. Selon de nombreuses dispositions légales existantes relatives à l'obligation de secret professionnel des praticiens de santé, la conservation et l'utilisation des dossiers des patients sont généralement limitées à la relation bilatérale directe entre le patient et le professionnel de santé/l'établissement de soins de santé.

d) Comme l'article 8, paragraphe 3, de la directive prévoit une dérogation à l'interdiction générale de traiter les données sensibles, il doit être interprété strictement.

e) À la question de savoir si l'article 8, paragraphe 3, de la directive pourrait constituer l'*unique* base juridique du traitement des données à caractère personnel dans un système de DME, le groupe de travail «Article 29» répond que l'article 8, paragraphe 3, ne peut concerner que le traitement de données médicales aux seules fins médicales et de soins de santé qui y sont mentionnées, et uniquement à la double condition que le traitement des données soit «nécessaire» et effectué par un praticien de santé ou par une autre personne soumise au secret professionnel ou à une obligation de secret équivalente. Lorsque le traitement des données à caractère personnel contenues dans un DME va au-delà de ces objectifs ou ne remplit pas cette double condition, l'article 8, paragraphe 3, ne peut servir de base juridique unique au traitement de ces données à caractère personnel.

Cependant, même si toutes ces conditions préalables étaient remplies, le groupe de travail «Article 29» tient à faire remarquer que les systèmes de DME créent de nouveaux risques, qui appellent de nouvelles sauvegardes en contrepartie: les systèmes de DME donnent un accès direct à un ensemble de documents concernant le traitement médical d'une personne donnée, qui portent sur toute une vie et proviennent de différentes sources (par exemple les hôpitaux, les professionnels de santé). Ces systèmes dépassent donc les frontières traditionnelles de la relation directe entre le patient et un professionnel de santé ou un établissement de soins de santé. La conservation d'informations médicales dans un DME va au-delà des méthodes traditionnelles de conservation et d'utilisation des documents médicaux ayant trait aux patients. Sur le plan technique, de multiples points d'accès sur un réseau ouvert tel que l'internet augmentent les risques d'interception de données relatives au patient. Le maintien de la norme juridique de confidentialité qui convient à des dossiers sur papier traditionnels peut s'avérer insuffisant pour protéger la vie privée d'un patient une fois que les dossiers médicaux électroniques sont mis en ligne. Des systèmes de DME pleinement opérationnels tendent donc à permettre et à faciliter l'accès aux informations médicales et aux données à caractère personnel sensibles. Faire en sorte que seuls les praticiens de santé habilités aient accès aux informations à des fins légitimes liées au traitement médical de la personne concernée représente un lourd défi pour ces systèmes. Ceux-ci rendent plus complexe le traitement des données à caractère personnel sensibles, avec des implications directes pour les

droits des personnes. Par conséquent, un système de DME est à considérer comme posant de nouveaux risques pour la protection des données à caractère personnel sensibles.

La garantie principale et traditionnelle prévue à l'article 8, paragraphe 3 – outre la limitation des finalités et le critère de stricte nécessité – est l'obligation de confidentialité imposée aux professionnels de la médecine à l'égard des données médicales relatives à leurs patients. Elle peut ne plus être pleinement applicable en cas de DME, puisque l'un des objectifs du DME est de mettre les professionnels qui n'ont pas participé au traitement médical précédent consigné dans un fichier médical en mesure d'accéder aux documents médicaux à des fins de traitement.

Par conséquent, le groupe de travail «Article 29» n'est pas convaincu que, même si l'article 8, paragraphe 3, est utilisé pour justifier le traitement des données, l'obligation de secret professionnel assure à elle seule une protection suffisante en cas de DME. De nouveaux risques appellent des garanties supplémentaires, voire nouvelles, par rapport à celles qui sont requises par l'article 8, paragraphe 3, afin d'assurer une protection suffisante des données à caractère personnel dans un contexte de DME.

7. L'article 8, paragraphe 4: dérogations pour motif d'intérêt public important

Plusieurs dispositions de la directive ménagent une marge de manœuvre importante, afin d'établir un juste équilibre entre la protection des droits de la personne concernée, d'une part, et les intérêts légitimes des responsables du traitement des données et des tiers et l'éventuel intérêt public, d'autre part.

L'article 8, paragraphe 4, de la directive permet aux États membres de prévoir d'autres dérogations à l'interdiction du traitement de catégories de données sensibles:

> *«Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.»*
>
> Le considérant 34 est libellé comme suit:
>
> *«(34) considérant que les États membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale - particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie - et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes;»*

a) Par conséquent, si un État membre entend faire usage de cette possibilité, la dérogation doit être inscrite dans une disposition légale ou une décision de l'autorité de contrôle (**base juridique spéciale**).

b) Ce traitement de données à caractère personnel sensibles doit être justifié par un motif d'**intérêt public important**. Le considérant 34 de la directive cite des exemples de domaines dans lesquels des cas d'«intérêt public important» sont particulièrement susceptibles de se manifester. Il s'agit de la santé publique et de la sécurité sociale, dans le but d'assurer la

qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie.

Il faut dans chaque cas que l'ensemble du traitement de données faisant l'objet de la dérogation présente un intérêt public important pour l'État membre et que ce traitement soit nécessaire à la lumière de cet intérêt public important. Toute mesure de ce type doit être proportionnée, c'est-à-dire qu'aucune autre mesure moins dérogatoire ne doit être disponible.

En outre, pour que toute atteinte au droit à la vie privée et de famille soit légitime, elle doit être conforme à l'article 8 de la convention européenne des droits de l'homme et doit être interprétée à la lumière de la jurisprudence de Strasbourg: elle doit être *«prévue par la loi»* et être *«nécessaire dans une société démocratique»* à des fins d'intérêt public. La Cour de Strasbourg a indiqué à plusieurs reprises que la loi autorisant l'ingérence *«doit indiquer la portée d'un tel pouvoir discrétionnaire conféré aux autorités compétentes ainsi que les modalités de son exercice de manière suffisamment claire, vu l'objectif légitime de la mesure en question, afin de conférer à l'individu une protection appropriée contre les ingérences arbitraires.»*

c) Les États membres sont tenus de prévoir des **garanties spécifiques et appropriées** afin de protéger les droits fondamentaux et la vie privée des personnes dans ce contexte.

d) Tout recours à l'article 8, paragraphe 4, par un État membre doit être **notifié à la Commission**, conformément à l'article 8, paragraphe 6, de la directive.

S'agissant des DME, le groupe de travail «Article 29» note que les arguments en faveur de l'introduction de systèmes de DME (cf. le point I ci-dessus) peuvent faire état d'«intérêts publics importants». Dans certains États membres, le «droit à la protection de la santé» est consacré dans la Constitution, ce qui montre l'importance attribuée à tous les moyens appropriés d'assurer la «protection de la santé». Dans de tels environnements juridiques, un système de DME serait certainement fondé sur l'«intérêt public important», puisqu'il s'agit d'un instrument essentiellement destiné à garantir une assistance médicale adéquate aux patients.

L'article 8, paragraphe 4, de la directive pourrait donc servir de base juridique à des systèmes de DME, pour autant que toutes les conditions qui y sont mentionnées soient remplies. Il faut en particulier prévoir des garanties appropriées pour la protection des données à caractère personnel.

Dans le chapitre suivant, le groupe de travail examinera les garanties possibles et le cadre juridique approprié pour les systèmes de DME.

III. Réflexions sur un cadre juridique approprié pour les systèmes de DME

Le groupe de travail «Article 29» développera ci-après les aspects pour lesquels des garanties spéciales[16] semblent particulièrement nécessaires dans les systèmes de DME afin de garantir les droits des patients à la protection des données. Vu l'incidence des systèmes de DME et le

[16] Les conditions générales prévues dans la directive 95/46/CE pour le traitement licite des données à caractère personnel ne sont pas répétées dans cette partie du document, puisqu'elles s'appliquent en tout état de cause. Le présent chapitre ne développe que les exigences supplémentaires spécifiques afférentes au traitement des données médicales dans les systèmes de DME qui semblent nécessaires pour compenser les risques spécifiques que les systèmes de DME présentent pour la vie privée.

besoin particulier d'en assurer la transparence, les garanties devraient de préférence être établies dans un cadre juridique complet spécifique.

1. Le respect de l'autodétermination

Même si un système de DME n'a pas que le consentement pour base juridique (article 8, paragraphe 2), la détermination par le patient lui-même de quand et comment ses données sont utilisées devrait constituer une garantie majeure[17].

a) L'«accord» du patient en présence de garanties appropriées est différent de son «consentement» en vertu de l'article 8, paragraphe 2, de la directive et n'a donc pas à satisfaire à toutes les exigences de l'article 8, paragraphe 2: par exemple, si le **consentement en tant que base juridique** du traitement de données relatives à la santé doit toujours être «explicite» en vertu de l'article 8, paragraphe 2, l'**accord en tant que garantie** ne doit pas nécessairement être donné sous la forme d'un consentement préalable: la possibilité d'autodétermination pourrait également, en fonction de la situation, être conférée sous la forme d'un droit de refus.

b) Différents types d'informations relatives à la santé ayant un potentiel de préjudice variable, il y a lieu de distinguer des catégories d'utilisation assorties de **degrés différents de possibilité d'exercer l'autodétermination**:

les dispositions juridiques instituant un système de DME devraient poser en règle le consentement préalable du patient pour l'encodage de données dans un DME ou l'accès à ces données (en particulier pour le traitement de données susceptibles d'un usage plus préjudiciable, telles que des données psychiatriques, sur l'avortement, etc.[18]) et prévoir une option de refus pour les données moins confidentielles[19], de manière à garantir le degré de protection requis, d'une part, et la faisabilité et la souplesse nécessaires, de l'autre.

c) En principe, un **patient devrait toujours avoir la faculté, s'il le désire, d'interdire la communication** de ses données médicales, rassemblées par un professionnel de santé durant le traitement, à d'autres professionnels de santé.

Il faudrait également examiner comment la suppression de l'accès aux informations contenues dans un DME doit être traitée : doit-elle être masquée afin d'être indétectable, ou faut-il dans certains cas, qu'un message indique qu'il existe d'autres informations, mais qu'elles ne sont disponibles que dans des conditions bien précises?

d) Dans l'hypothèse que nul ne peut être contraint à participer à un système de DME, il faut que les dispositions juridiques établissant ce système prévoient le **retrait complet éventuel du système de DME.** Il convient de prévoir des règles déterminant si ce retrait entraîne l'obligation d'effacer complètement les données du système de DME ou simplement

---

17 Dans certains pays, il existe non seulement un droit fondamental à la protection des données, mais aussi un droit constitutionnel à une protection optimale de la santé: en conséquence, sur la base de cette obligation d'assurer un traitement optimal, certains États membres ont donné aux praticiens de santé un accès automatique aux données disponibles via le système de DME. Cela semble acceptable tant que l'équilibre nécessaire est assuré par l'importance conférée à d'autres garanties, telles qu'une réglementation détaillée des circonstances de l'accès légitime et les conséquences - graves - en cas d'utilisation abusive des droits d'accès, etc.

18 Des techniques particulières telles que des «enveloppes scellées», qui ne peuvent être ouvertes sans la coopération de la personne concernée, pourraient être utilisées.

19 Toutefois, pour que les solutions de refus constituent une «garantie appropriée» efficace, il faudrait que le patient reçoive des informations adéquates.

l'obligation d'empêcher l'accès à ces données ; le choix pourrait également être laissé à la personne concernée.

2. L'identification et l'authentification des patients et des professionnels de santé

a) L'identification fiable[20] **des patients** dans les systèmes de DME est d'une importance capitale. Si une d'erreur d'identification entraînait l'utilisation de données se rapportant à une autre personne, les conséquences seraient souvent néfastes.

Des cartes de santé à puce pourraient contribuer fortement à une identification électronique fiable des patients ainsi qu'à leur **authentification**[21] **s'ils veulent accéder aux données de leur propre DME.**

b) De plus, vu la grande sensibilité des données relatives à la santé, il est impératif que les personnes non autorisées ne puissent y accéder. Le contrôle fiable de l'accès dépend de la fiabilité de l'identification[22] et de l'authentification. Par conséquent, il est indispensable d'**identifier les utilisateurs de façon unique et de les authentifier correctement**[23].

L'un des principaux avantages des systèmes de DME étant la possibilité d'y accéder par voie électronique, quel que soit le moment ou l'endroit, des procédures d'identification et d'authentification électroniques fiables devront être mises au point. L'authentification au moyen de signatures électroniques – délivrées aux utilisateurs autorisés avec une identification officielle adéquate, par exemple sur des cartes à puce spéciales – devrait être envisagée du moins dans une perspective à long terme afin d'éviter les risques connus de l'authentification par mot de passe.

Pour le professionnel de santé, il faudra mettre au point un système d'identification et d'authentification qui prouve non seulement son identité, mais aussi **à quel titre il agit électroniquement** (en tant que psychiatre ou qu'infirmière, par exemple).

3. L'autorisation d'accéder aux DME pour lecture et écriture

a) Garanties générales relatives à l'accès

Les données contenues dans les systèmes de DME sont des dossiers médicaux confidentiels. Le **principe essentiel** régissant l'accès au DME doit donc être que – outre le patient lui-même – **seuls les professionnels de santé**/le personnel autorisé des établissements de soins de santé **qui interviennent en ce moment dans le traitement** du patient **peuvent y avoir accès**. Il doit exister une relation de traitement médical réel et actuel entre le patient et le professionnel de santé qui souhaite accéder à son DME.

---

[20] L'«identification» permet de décrire une personne au moyen d'identifiants tels que le nom, la date de naissance, l'adresse, etc.; dans le présent contexte, cette description devra être certifiée officiellement par un certificat de naissance, un passeport ou une carte de santé, etc.

[21] L'«authentification» permet de certifier que la personne qui déclare avoir une identité donnée est réellement cette personne. Elle se fait en général par la présentation d'un document d'identité officiel muni d'une photo (par exemple un passeport) ou, dans le monde électronique, par l'utilisation d'une signature électronique.

[22] L'«identification fiable» ne devrait pas faire usage de numéros d'identification qui sont très largement utilisés dans d'autres contextes sans garanties spécifiques, afin d'éviter de faciliter toute interconnexion (voir l'article 8, paragraphe 7, de la directive).

[23] En France, les premières expériences sur les DME qui sont sur le point de commencer reposent sur la création d'un identifiant spécifique; il n'est pas encore certain que ce système sera conservé dans la configuration définitive des DME.

Il semble également nécessaire de déterminer quelles catégories et quels niveaux de professionnels de santé/établissements de soins de santé peuvent accéder aux données des DME (médecins généralistes, médecins hospitaliers, pharmaciens, infirmières, chiropracteurs?, psychologues?, thérapeutes familiaux?, etc.).

La protection des données pourrait en outre être renforcée par des **droits d'accès modulaires**, c'est-à-dire en formant dans un système de DME des catégories de données médicales, en conséquence de quoi l'accès serait limité à des catégories spécifiques de professionnels de santé/établissements de soins de santé[24]. Les avantages éventuels d'une configuration modulaire des DME sont abordés plus longuement au point 6.

b) Garanties spéciales relatives à l'accès supposant la participation du patient

Si c'est faisable et possible, c'est-à-dire s'il est présent et capable d'agir, le patient devrait **avoir la faculté d'empêcher l'accès aux données de son DME s'il le souhaite**. Pour ce faire, il doit savoir au préalable qui désire accéder à ses données et pourquoi et quand, et être informé des éventuelles conséquences d'un refus d'accès. Il convient de prévoir des procédures permettant d'éviter que le patient ne soit indûment soumis à des pressions psychologiques pour accepter l'accès à ses données.

Lorsque la **preuve que le patient a donné son accord** à l'accès aux données de son DME est nécessaire, des instruments fiables à cet effet sont indispensables, tels que la vérification électronique du jeton du patient ou – si de tels instruments sont déjà généralement disponibles – la signature électronique du patient, etc. La présentation de cette preuve doit être documentée électroniquement en vue de contrôles éventuels.

Il y a également lieu de définir des règles stipulant si la personne concernée peut exiger que certaines données ne soient pas inscrites dans son fichier. Des «enveloppes scellées» qui ne peuvent être ouvertes sans le consentement explicite de la personne concernée pourraient être un moyen de régler cette question.

c) L'accès des personnes concernées aux données de leur propre DME:

L'octroi ou non aux patients d'un **accès (électronique) direct** à leur DME **à des fins de lecture uniquement** est une question de faisabilité médicale. Le droit d'accès associé à la protection des données, par exemple en vertu de l'article 12 de la directive 95/46/CE, ne doit pas nécessairement impliquer un accès *direct* en toutes circonstances. L'accès direct pourrait toutefois contribuer fortement à la confiance dans le système de DME. Du point de vue de la protection des données, une condition préalable à l'octroi de l'accès direct serait de sécuriser l'identification et l'authentification électroniques afin d'empêcher l'accès de personnes non autorisées.

Les dispositions relatives au système de DME devraient également déterminer si les **patients** doivent **inscrire les données dans leur DME** eux-mêmes ou les faire inscrire par un professionnel de santé. Une transparence suffisante des procédures d'encodage révélant l'auteur des inscriptions dans le DME permettrait très probablement de résoudre les éventuels problèmes de responsabilité de l'exactitude des données. On pourrait également envisager de limiter l'accès pour écriture à un module spécifique du DME.

[24] Par exemple, l'accès à des données afférentes à un traitement psychiatrique pourrait se limiter à un premier niveau aux psychiatres; ou bien un module spécial «médication» pourrait également être rendu accessible aux pharmaciens, qui n'auraient pas accès aux autres parties du système de DME.

Dans ce cadre, les capacités et les besoins particuliers des malades chroniques, des personnes âgées et des handicapés et des invalides doivent être pris en considération.

4. L'utilisation des DME à d'autres fins

L'acceptation des systèmes de DME par les citoyens dépendra de leur **confiance dans la confidentialité du système**.

La justification de l'accès légitime aux données d'un DME doit correspondre au but essentiel de tout système de DME, à savoir un bon traitement médical grâce à de meilleures informations. **Le groupe de travail est d'avis qu'il faut en principe interdire l'accès aux données médicales contenues dans les DME à d'autres fins que celles mentionnées à l'article 8, paragraphe 3.**

Cela exclurait par exemple l'accès aux DME des praticiens de la médecine qui agissent en tant qu'experts pour le compte de tiers: par exemple pour des compagnies d'assurance privées, dans des litiges, pour l'octroi de l'aide à la retraite, pour les employeurs de la personne concernée, etc. En outre, le droit disciplinaire applicable aux professionnels de santé devrait être conçu de façon à combattre efficacement les infractions à ces règles.

Des mesures spéciales devraient être arrêtées pour empêcher que les patients ne soient illégalement incités à communiquer les données de leur DME, par exemple à la demande d'un éventuel futur employeur ou d'une compagnie d'assurance privée. Il est essentiel que les patients en soient informés pour éviter qu'ils ne cèdent à de telles demandes de divulgation, qui seraient illégales en vertu de la législation sur la protection des données. Il faudrait peut-être aussi appliquer des moyens techniques, notamment des exigences spéciales pour l'impression de l'intégralité d'un DME, etc.

Le traitement des données des DME aux fins de la **recherche scientifique médicale et des statistiques gouvernementales** pourrait être autorisé en tant qu'exception à la règle exposée ci-dessus, pour autant qu'il soit conforme à la directive (cf. article 8, paragraphe 4, et le considérant 34): les exceptions doivent donc être prévues par la loi à des fins spécifiques et prédéterminées, dans des conditions spéciales garantissant la proportionnalité («garanties spécifiques et appropriées») de façon à protéger les droits fondamentaux et la vie privée des personnes.

De surcroît, les données des systèmes de DME ne devraient, dans la mesure du possible, être utilisées à d'autres fins (par exemple, pour les statistiques ou l'évaluation de la qualité) que sous forme anonyme, ou du moins au moyen d'une pseudonymisation sûre[25].

5. La structure organisationnelle d'un système de DME

Dans le cadre du débat sur les différentes possibilités organisationnelles de stockage des données dans un système de DME, les principales solutions suivantes sont généralement citées:

- le DME en tant que système donnant accès aux dossiers médicaux conservés par le professionnel de santé, qui est tenu de conserver des dossiers sur le traitement de ses patients – souvent appelé **«stockage décentralisé»**; ou

[25] La pseudonymisation consiste à transposer les identifiants (tels que le nom, la date de naissance, etc.) sous une nouvelle désignation, de préférence par cryptage, afin que le destinataire des informations ne puisse pas identifier la personne concernée.

- le DME en tant que système de stockage uniforme vers lequel les professionnels de santé doivent transférer leurs documents - souvent appelé **«stockage centralisé»**;

- une troisième solution pourrait consister à permettre à la personne concernée d'être le «maître» de son propre dossier électronique en lui offrant le stockage de ses propres données médicales en tant que service en ligne spécial sous son propre contrôle, et en lui donnant même éventuellement le pouvoir de décider des données à faire figurer dans le DME[26].

a) Si la troisième solution **(stockage sous le contrôle de la personne concernée)** semble être la meilleure en termes d'autodétermination, l'exactitude et l'exhaustivité de cette documentation pourraient poser des problèmes si la personne concernée est seule à décider des données à conserver dans son DME et qu'aucune intervention d'un professionnel de santé n'est intégrée dans le système.

b) Dans le cas du modèle de **stockage «décentralisé»**, qui ne devient un «système» que par la création de chemins de recherche correspondants, la structure de documentation des données relatives à la santé chez les prestataires de soins de santé resterait inchangée. La facilité de localisation des données d'un patient dans ce système dépend de la qualité du système de recherche.

Dans ce modèle organisationnel, le **professionnel de santé/l'établissement de soins de santé reste le «responsable»** du fichier (plus précisément: de la partie du DME qu'il a créée). Vu l'architecture complexe de ce modèle, il pourrait se révéler nécessaire de désigner un organe central chargé de gérer et de contrôler l'ensemble du système et d'en assurer la compatibilité avec la protection des données. Il pourrait également être utile que les personnes concernées puissent soumettre leurs problèmes de protection des données à un organe central plutôt que de devoir chercher parmi une multitude de responsables.

c) Le principal avantage d'un système de **stockage «centralisé»** serait vraisemblablement l'amélioration de la sécurité technique et de la disponibilité (accès 24h/24), qui ne sont pas si faciles à garantir si le système de DME s'étend au delà des hôpitaux. L'ensemble du système relèvera d'un seul responsable distinct des professionnels de santé/établissements de soins de santé qui ont transmis leur documentation (en tout ou en partie) au système central.

En termes de protection des données, on pourrait reprocher à un système de ce genre d'accroître potentiellement le risque d'abus de données faisant l'objet d'un stockage centralisé. On pourrait prévoir des dispositifs particuliers et des mesures de sécurité (par exemple le stockage crypté) pour compenser, du moins en grande partie, les risques posés par la centralisation des données. Toutefois, la responsabilité de la confidentialité échappe alors aux professionnels de la médecine, ce qui pourrait influer sur la confiance des patients dans le système.

La possibilité pour le patient d'influencer le contenu et la communication de son DME dépendrait dans les deux cas – stockage décentralisé et centralisé – de la configuration particulière du système (voir le point 3 b).

[26] C'est le modèle français qui est actuellement mis en place. Ces prestataires de services sont appelés «hébergeurs» et leur statut est régi par un décret qui a fait l'objet d'un avis préalable de la CNIL. Il est complexe et est axé sur l'accréditation des prestataires de services et sur la sécurité du système.

6. Les catégories de données stockées dans les DME et leurs modes de présentation

L'idée fondamentale d'un «système de DME» est de collecter toutes les données relatives à la santé d'une personne donnée qui sont susceptibles d'être utiles à long terme, de sorte qu'en cas de traitement ultérieur, des informations complètes et pertinentes soient disponibles et que les patients aient une meilleure chance de se voir administrer un traitement efficace.

Le groupe de travail considère que cela pourrait entraîner les principaux problèmes suivants:

a) L'«**exhaustivité» d'un fichier médical** est pratiquement impossible et n'est pas non plus souhaitable: **seules les informations *pertinentes* doivent être inscrites dans le DME**. L'une des questions les plus difficiles lors de l'établissement d'un système de DME sera donc de déterminer quelles catégories de données médicales doivent être collectées dans un DME et pendant combien de temps elles doivent être conservées[27]. Bien que la réponse à cette question appartienne avant tout aux experts en médecine, il y va également de la protection des données: selon les principes de pertinence et de proportionnalité de la collecte de données, toute compilation de données doit se limiter aux données qui sont pertinentes et non excessives au regard de la finalité du traitement de données (article 6, paragraphe 1, point c), de la directive). La légitimité des systèmes de DME dépendra donc aussi du choix des «bonnes» catégories de données et de la «bonne» durée de conservation des informations dans le DME.

b) Concernant la présentation des données dans les DME: le fait qu'il soit possible de distinguer différentes catégories de données relatives à la santé qui nécessitent des degrés de confidentialité très différents donne à penser qu'il pourrait s'avérer utile de créer, au sein du système de DME, différents **modules de données**, assortis de conditions d'accès différentes: un module de données «vaccination» devrait être accessible à tout moment à la personne concernée et pourrait également être accessible à un grand nombre de membres du personnel des services de santé; un module de données «médication» pourrait être doté d'un accès spécial pour les pharmaciens si le patient y consent[28]; un module de données d'«urgence» pourrait être doté de moyens d'accès techniques spéciaux, etc. La création de modules pour des «systèmes de rappel» spéciaux semblerait également utile; ils permettraient de rappeler automatiquement à un patient les vaccins, les bilans de santé et les examens de suivi nécessaires.

Les données particulièrement sensibles pourraient également être mieux protégées par un stockage dans des modules séparés, assorti de conditions d'accès très strictes; ce serait le cas notamment des données sur le traitement psychiatrique, sur le VIH ou sur l'avortement. Au lieu d'exclure ces données du DME – ce qui pourrait nuire à l'efficacité de futurs traitements médicaux -, le système devrait prévoir des restrictions spéciales d'accès à ces données, dont le consentement explicite du patient et des méthodes de protection techniques spécifiques (telles que les «enveloppes scellées»).

c) Pour la configuration des dossiers DME, il faudra également tenir compte des **demandes d'informations spéciales** récurrentes. Par exemple, en vertu de la législation nationale, les

---

[27] Certaines catégories de données sont importantes tout au long de la vie d'un patient (par exemple les allergies), tandis que d'autres ne sont extrêmement importantes que pendant un bref laps de temps, notamment les incompatibilités de traitements.

[28] L'avantage de disposer d'un tel module de médication au sein du DME serait double, en ce sens qu'il donnerait également au médecin traitant la possibilité de prendre connaissance de toute la médication prescrite au patient.

compagnies d'assurance privées pourraient être en droit de recevoir si nécessaire certaines informations (limitées) concernant les dossiers médicaux afin de remplir leurs obligations contractuelles envers les patients assurés. Comme il semble inacceptable de permettre aux compagnies d'assurance privées d'accéder au DME d'un patient, une solution pourrait consister à établir un dossier spécial normalisé, répondant en cas de besoin aux demandes d'informations légitimes de l'assureur et qui, si le patient y consent, pourrait être transmis (électroniquement) à la compagnie d'assurance privée.

7. Le transfert international des dossiers médicaux

La mise à disposition par voie électronique des données médicales contenues dans les systèmes de DME peut améliorer considérablement les possibilités de diagnostic et de traitement en permettant le recours à une expertise médicale uniquement disponible dans des établissements médicaux étrangers. La consultation d'experts étrangers afin de poser un diagnostic ne nécessite généralement pas la divulgation de l'identité du patient. Ces données ne devraient donc si possible être transférées à des pays non membres de l'Union européenne/de l'Espace économique européen que **sous forme anonyme ou, du moins, pseudonymisée**. Si la personne concernée n'a pas donné son consentement explicite au transfert des données à caractère personnel[29], cela éviterait également de devoir obtenir sa permission, puisqu'elle ne pourrait être identifiée par le destinataire.

Vu le risque élevé qui pèse sur les données à caractère personnel contenues dans un système de DME dans un environnement dépourvu de protection adéquate, le groupe de travail «Article 29» tient à souligner que tout traitement – en particulier le stockage – de données des DME doit avoir lieu dans des pays qui appliquent la directive européenne sur la protection des données ou un cadre juridique adéquat de protection des données.

Les échanges transfrontaliers de données dans le cadre d'études cliniques posent un problème spécifique: le groupe d'étude qui se charge directement des patients pourrait parfois avoir besoin d'accéder aux données des DME sous leur forme personnalisée initiale. Pour tout transfert de données résultant d'études cliniques aux commanditaires ou à d'autre institutions qui y sont licitement associées, une pseudonymisation sûre doit toutefois être requise en tant que condition minimale, en particulier si ces commanditaires sont établis dans des pays n'assurant pas une protection adéquate des données.

Dans ce cadre, il convient toujours d'accorder une attention particulière aux aspects relatifs à la sécurité des données afin d'éviter les risques de divulgation non autorisée dans des environnements qui ne garantissent peut-être pas une protection suffisante des données.

8. La sécurité des données

L'acceptabilité d'un système de traitement des données présentant un potentiel de risque exceptionnel dépend d'un niveau de sécurité des données suffisamment élevé dans l'ensemble du système. **L'accès des personnes non autorisées doit être virtuellement impossible et empêché** pour que le système soit acceptable du point de vue de la protection des données. En revanche, l'accès des professionnels habilités en cas de réel besoin de ces informations doit être pratiquement illimité si l'on veut que le système produise les avantages promis pour le traitement médical des patients.

---

[29] Lorsque le patient est physiquement incapable de répondre à une demande de consentement (par exemple parce qu'il est dans le coma), ses données médicales peuvent néanmoins, conformément à l'article 26, paragraphe 1, point e), de la directive, être transférées à des pays sans protection adéquate des données si ses intérêts vitaux le requièrent.

Le cadre juridique instituant un système de DME devrait prévoir l'application d'une série de mesures techniques et organisationnelles visant à éviter la perte de données, la modification ou le traitement non autorisés de données ou l'accès non autorisé aux données dans le système de DME. L'intégrité du système doit être garantie par l'usage des connaissances et des instruments représentant l'état actuel de la technique en sciences de l'informatique et en technologies de l'information.

Les technologies de protection de la vie privée (PET)[30] doivent être appliquées autant que possible afin de promouvoir la protection des données à caractère personnel. Le cryptage ne devrait pas être utilisé uniquement pour le transfert, mais aussi pour le stockage des données dans les systèmes de DME. Toutes les mesures de sécurité devraient être conviviales pour les utilisateurs afin d'en généraliser l'application. Les coûts nécessaires sont à considérer comme un investissement dans la compatibilité des systèmes de DME avec les droits fondamentaux, qui sera l'une des conditions les plus importantes du succès de ces systèmes.

Indépendamment du fait que nombre des garanties évoquées ci-dessus comportent déjà des éléments de sécurité des données, le cadre juridique concernant les mesures de sécurité devrait prévoir en particulier la nécessité:

- d'un système fiable et efficace d'identification et d'authentification électroniques ainsi que de registres constamment mis à jour pour vérifier si les personnes qui ont ou demandent l'accès au système de DME disposent de l'autorisation nécessaire;

- de l'enregistrement et de la documentation exhaustifs de toutes les étapes de traitement qui ont eu lieu dans le système, en particulier les demandes d'accès pour lecture ou écriture, assortis de contrôles internes réguliers et du contrôle de l'authenticité de l'autorisation;

- de mécanismes efficaces de sauvegarde et de récupération afin de protéger le contenu du système;

- de l'impossibilité d'accéder sans autorisation aux données des DME ou de les modifier au moment du transfert ou du stockage des sauvegardes, par exemple en utilisant des algorithmes cryptographiques;

- d'instructions claires et documentées à tout le personnel autorisé au sujet de l'utilisation correcte des systèmes de DME et de la façon d'éviter les risques de sécurité et les atteintes à la sécurité;

- d'une nette distinction des fonctions et compétences des catégories de personnes qui sont chargées du système, ou du moins qui y participent, afin de pouvoir déterminer les responsables en cas de problème;

- de contrôles internes et externes réguliers en matière de protection des données.

9. La transparence

Il semble évident qu'un DME offre de grandes possibilités pour le traitement médical, mais présente également en principe un risque élevé d'abus par un accès non autorisé. Pour faire confiance au système de DME, l'opinion et les citoyens réclameront donc une **transparence**

[30] À ce sujet, voir le point 4.3 du «Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)» de la Commission, COM (2003) 265 final.

accrue en ce qui concerne son contenu et son fonctionnement. La **notification** aux autorités de contrôle de la protection des données, assortie d'**informations spéciales, facilement disponibles et compréhensibles**, doit être effectuée par le(s) responsable(s) du système. L'utilisation de l'internet en tant que canal idéal de diffusion de l'information pourrait contribuer à garantir la transparence nécessaire du ou des système(s) de DME mis en place au niveau national.

Des points d'accès gratuits et conviviaux mais sûrs permettant aux personnes concernées de vérifier le contenu et la communication de leur DME pourraient également constituer une contribution précieuse à la transparence et, partant, à la confiance dans le système.

10. Les questions de responsabilité

Tout système de DME doit également garantir que le risque d'**atteintes à la vie privée** dû au stockage de données médicales et à la fourniture de ces données soit adéquatement contrebalancé **par la responsabilité pour le préjudice** causé, par exemple par l'utilisation incorrecte ou non autorisée de données des DME.

L'analyse des problèmes que les systèmes de DME peuvent poser du point de vue de la protection des données ne peut évoquer que superficiellement les questions de la responsabilité en cas d'utilisation incorrecte. De l'avis du groupe de travail, tout État membre désirant instaurer un système de DME doit mener minutieusement au préalable des études approfondies de droit civil et médical réalisées par des experts et des évaluations d'impact pour clarifier les nouvelles questions de responsabilité susceptibles de se poser dans ce contexte, notamment en ce qui concerne l'exactitude et l'exhaustivité des données inscrites dans le DME, la définition du degré de connaissance qu'un professionnel de santé traitant un patient doit avoir du DME de celui-ci ou les conséquences prévues par le droit de la responsabilité si l'accès est indisponible pour des raisons techniques, etc.

11. Les mécanismes de contrôle du traitement des données contenues dans les DME

Vu les **risques particuliers** engendrés par la création de systèmes de DME, des **mécanismes de contrôle efficaces** sont nécessaires pour évaluer les garanties existantes. La complexité des informations contenues dans un DME, associée à la multitude d'utilisateurs possibles, peut nécessiter de nouvelles procédures concernant les droits d'accès des personnes concernées:

a) une **procédure d'arbitrage spéciale** devrait être instituée **pour les litiges relatifs** à l'utilisation correcte des données contenues dans les systèmes de DME; les personnes concernées devraient pouvoir recourir à cette procédure facilement et gratuitement. Étant donné qu'une expertise médicale spéciale sera souvent nécessaire pour apprécier les recours concernant des informations erronées ou inutilement traitées dans les systèmes de DME, les autorités de contrôle de la protection des données pourraient ne pas être les mieux placées pour connaître de ces recours, du moins pas en première instance. Les «défenseurs des patients» pourraient, là où ils existent déjà, être chargés de cette tâche;

b) un système de DME doit permettre à la personne concernée d'exercer ses droits d'accès sans difficultés indues. En principe, c'est le responsable du traitement des données qui est obligé d'accorder l'accès. **Les systèmes de DME sont** toutefois **des systèmes de mise en commun d'informations** qui comptent de nombreux responsables du traitement des données. Dans ces conditions, **une seule institution spéciale doit être responsable envers les personnes concernées du traitement correct des demandes d'accès**. Vu la complexité

prévisible d'un DME pleinement opérationnel et la nécessité de faire en sorte que les patients aient confiance dans le système, il semble essentiel que les patients dont les données sont traitées dans un DME sachent comment contacter un partenaire responsable avec lequel ils peuvent discuter des éventuelles lacunes du système. Des dispositions spéciales à cet effet devront être incluses dans tout règlement sur les systèmes de DME;

c) afin de susciter la confiance, une **procédure spéciale visant à informer les personnes concernées de l'identité de ceux qui ont accédé à leur DME et de la date de cet accès pourrait être instaurée**. La fourniture à intervalles réguliers d'une liste des personnes ou institutions qui ont eu accès à leur dossier rassurerait les patients quant à leur capacité de savoir ce qu'il advient de leurs données dans le système de DME;

d) il faut prévoir **des contrôles internes et externes réguliers des listes d'accès**. La liste annuelle des accès susmentionnée envoyée aux personnes concernées constituerait un moyen efficace supplémentaire de vérifier la légalité de l'utilisation des données des DME. La désignation d'agents chargés de la protection des données dans les hôpitaux participant aux systèmes de DME améliorerait certainement la probabilité d'une utilisation correcte des données contenues dans ces systèmes.

IV. CONCLUSION

Toutes les personnes et tous les patients ont le droit à la vie privée et sont donc normalement fondés à attendre de tous les professionnels de santé qu'ils respectent rigoureusement la confidentialité et la protection de leurs informations personnelles. Ce droit existe également pour les systèmes de dossiers médicaux électroniques (DME).

Le groupe de travail «Article 29» a élaboré le présent document de travail afin de donner des indications au sujet de l'interprétation du cadre juridique de protection des données applicable aux systèmes de dossier médical électronique (DME) et de dégager quelques principes généraux. Ce document de travail vise également à exposer les conditions en matière de protection des données qui doivent constituer le préalable à la création d'un système de DME national ainsi que les garanties applicables, et à contribuer à l'application uniforme des mesures nationales adoptées en vertu de la directive 95/49/CE.

Le groupe de travail «Article 29» souligne que la création et le fonctionnement des systèmes de DME doivent respecter pleinement les principes de protection des données à caractère personnel consacrés par la directive 95/46/CE. Il considère que le respect de ces principes aide toutes les personnes et institutions concernées à assurer le bon fonctionnement de ces systèmes. Il insiste en outre sur la nécessité d'inscrire la création et le fonctionnement des systèmes de DME dans un cadre juridique bien conçu, doté de garanties visant à protéger les données à caractère personnel, quelle que soit la base juridique de ces systèmes.

Le groupe de travail «Article 29» invite le corps médical, tous les autres professionnels de santé et toutes les autres personnes et institutions intervenant dans la fourniture de services médicaux ainsi que la population en général à formuler des commentaires sur le présent document de travail[31].

[31] Vous pouvez envoyer vos commentaires sur le présent document de travail au secrétariat du groupe de travail «Article 29»:
Commission européenne, direction générale «Justice, liberté et sécurité»

À la lumière de l'évolution en cours dans le domaine, d'autres travaux, des commentaires supplémentaires et un suivi par le groupe de travail «Article 29» pourraient s'avérer nécessaires.

Fait à Bruxelles, le 15 février 2007

Pour le groupe de travail

Le président

Peter SCHAAR

Unité C.5 – Protection des données
Bureau: LX 46 1/43
B - 1049 Bruxelles
E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu; fax (32-2) 299 80 94

Tous les commentaires des secteurs public et privé seront publiés sur le site internet du groupe de travail «Article 29», à moins que les répondants n'indiquent explicitement que certaines informations doivent rester confidentielles.