Introduction au régime juridique du traitement informatisé des données du patient à des fins thérapeutiques dans un service des urgences hospitalier

Herveg, Jean; Poullet, Yves

Published in:
Urgence aux urgences

Publication date:
2004

Document Version
le PDF de l'éditeur

Chapitre 2

Introduction au régime juridique du traitement informatisé des données du patient à des fins thérapeutiques dans un service des urgences hospitalier

Jean HERVEG
Yves POULLET
Centre de Recherche Informatique et Droit (CRID)
Facultés Universitaires Notre-Dame de la Paix, Namur
yves.poullet@fundp.ac.be

Introduction

L'informatisation d'un service des urgences hospitalier implique fréquemment le recours à des outils informatiques, voire télématiques, pour gérer tout ou partie des données des patients pris en charge.

La gestion informatisée totale ou partielle des données du patient s'inscrit dans une ou plusieurs finalités à définir dans chaque cas d'espèce. Ainsi, si l'outil informatique vient en support à l'octroi de soins au patient, la finalité poursuivie par son implantation et son utilisation sera « thérapeutique » ou de « soins de santé ». Si l'informatisation de ses données participe à la gestion des aspects administratifs de la prise en charge du patient, la finalité poursuivie par le traitement de données sera « administrative ». D'autres finalités peuvent être assignées et poursuivies telles que les finalités statistiques, scientifiques, de contrôle de la qualité des soins, etc.

Toutes les opérations informatiques (encodage, codage, transmission, lecture, destruction, correction, etc.) effectuées sur des données à caractère personnel du patient et qui se rattachent à une même finalité, constituent un traitement de données à caractère personnel particulier. Il y a donc autant de traitements de données que de finalités poursuivies. Plusieurs finalités peuvent coexister sous certaines conditions.

Le traitement de données à caractère personnel[2] du patient à des fins thérapeutiques obéit aux règles posées par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (loi "vie privée") et à son arrêté royal d'exécution du 13 février 2001, mais aussi, en outre, aux règles spécifiques relatives à chaque finalité et situation envisagées, telles que les règles relatives au secret médical, l'arrêté royal n° 78 relatif à l'exercice des professions des soins de santé, la loi du 7 août 1987 sur les hôpitaux, la loi relative aux droits du patient, les règles déontologiques, etc.

La présente communication se propose d'identifier les principaux acteurs du traitement informatisé de données à caractère personnel du patient à des fins thérapeutiques dans un service des urgences hospitalier, et de décrire leurs rôles :

1° Le responsable du traitement des données du patient ;
2° Le sous-traitant du responsable du traitement ;
3° Le professionnel de la santé sous la responsabilité et la surveillance duquel doit s'effectuer le traitement de données à caractère personnel relatives à la santé ;
4° Le conseiller en sécurité ;
5° Le patient.

I. Le responsable du traitement des données du patient

I.1 Détermination du responsable du traitement des données du patient

Le responsable du traitement des données à caractère personnel du patient est « (...) la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel » (art. 1, § 4, loi "vie privée").

Sa détermination est cruciale puisqu'il est responsable du respect de la presque totalité des obligations imposées par ou en vertu de la loi "vie privée".

[2] Données à caractère personnel et données à caractère personnel relatives à la santé. Ces deux catégories de données répondent à un ensemble de règles communes ; cependant, des règles spécifiques s'appliquent en outre aux données à caractère personnel relatives à la santé.

Aucune disposition légale ou réglementaire spécifique n'indique qui, au sein de l'hôpital, est le responsable du traitement des données du patient à des fins thérapeutiques. Il convient néanmoins de tenir compte du fait que la loi du 7 août 1987 sur les hôpitaux confie au gestionnaire de l'hôpital la responsabilité générale et finale pour l'activité hospitalière, sur le plan de l'organisation et du fonctionnement, ainsi que sur le plan financier. Ce gestionnaire a également la charge de définir la politique générale de l'hôpital et de prendre les décisions de gestion. Il serait donc logique que le gestionnaire de l'hôpital soit le responsable du traitement des données du patient au sein de l'hôpital ou qu'à tout le moins, il désigne la personne devant assumer cette fonction en son nom et pour son compte. Ceci est néanmoins sans préjudice du fait que la personne qui aura concrètement, dans les faits, déterminé les finalités et les moyens d'un traitement de données, en sera le responsable pour l'application de la loi "vie privée".

Par ailleurs, il serait opportun que la détermination des finalités et des moyens du traitement des données du patient se fasse en concertation avec les autres personnes ou organes de l'hôpital impliqués dans celle-ci. Cela vise tant le directeur de l'hôpital, que le directeur médical, les médecins chefs, les infirmiers en chef, le conseil médical, le conseil infirmier et paramédical, le service informatique de l'hôpital, éventuellement le comité d'éthique hospitalier, sans omettre les utilisateurs du logiciel (soit le personnel soignant).

I.2 Les fonctions du responsable du traitement des données du patient

I.2.1. Vérification des conditions de légitimité et licéité du traitement des données (article 4, §1, 1° et 2 ° de la loi "vie privée")

Le responsable du traitement doit vérifier la légitimité et la licéité du traitement de données envisagé.

a. La légitimité du traitement des données du patient

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. Si le traitement doit correspondre à une hypothèse visée à l'article 5 de la loi "vie privée" (consentement de la personne concernée, exécution d'un contrat, obligation légale du responsable du traitement,

sauvegarde de l'intérêt vital de la personne concernée, exécution d'une mission d'intérêt public, réalisation d'un intérêt légitime), la balance des intérêts en présence doit toutefois être réalisée dans chaque cas d'espèce en fonction de la finalité concrètement envisagée pour s'assurer de la légitimité réelle du traitement informatisé de données du patient.

En outre, la loi "vie privée" prohibe le traitement des données à caractère personnel relatives à la santé du patient sauf dans certaines hypothèses spécifiques ; ainsi, par exemple, « lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé » (article 7, § 2, j, de la loi). Cette hypothèse correspond formellement à la finalité poursuivie par la gestion informatisée de données du patient dans un service des urgences hospitalier en support à l'octroi de soins de santé.

A cet égard, si le traitement informatisé de données du patient d'un service d'urgences apparaît *a priori* formellement légitime, le responsable du traitement doit encore vérifier si le traitement des données envisagé répond à la condition de la *proportionnalité* : il devra s'assurer qu'il n'y a pas une disproportion entre, d'une part, l'intérêt et les avantages apportés par le traitement informatisé et, d'autre part, les atteintes (ou risques d'atteintes) aux droits fondamentaux des patients dont on traitera les données.

Enfin, les données du patient ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités annoncés au patient.

b. La licéité du traitement des données du patient

Le traitement informatisé de données à caractère personnel du patient doit être licite ; à cet effet, il doit respecter toutes les dispositions légales et réglementaires spécifiques qui le concernent.

L'obligation légale au secret médical des praticiens retient spécialement l'attention.

Cette obligation se justifie par l'exigence de confiance qui doit régner entre le patient et le praticien qui le soigne. Le secret médical vise non seulement à protéger les intérêts individuels du patient mais également l'intérêt de la société en permettant à chaque citoyen de bénéficier de soins avec la garantie que ses confidences seront respectées.

L'obligation au secret concerne les praticiens professionnels intervenant dans une relation de soins (médecins, infirmières, kinésithérapeutes, ...) mais aussi tous leurs collaborateurs obligés, en l'occurrence les secrétaires, téléphonistes, stagiaires, ambulanciers du service 100, sans excepter le personnel du service d'accueil hospitalier...

L'interdiction de divulguer des données à des tiers ne peut être levée que dans des hypothèses strictement déterminées, à savoir, au regard de l'article 458 du Code pénal, lorsque la loi contraint le dépositaire à révéler le secret ou en cas de témoignage en justice.

Le Code de déontologie médicale donne une description précise et complète du secret professionnel médical (art. 56 et s.). Sous cet angle, le champ d'application du secret médical est large puisqu'il interdit au médecin de révéler à quiconque ce qu'il a constaté, vu, connu, appris, découvert ou surpris dans l'exercice ou à l'occasion de l'exercice de sa profession.

L'article 58 du Code de déontologie médicale reprend les différentes exceptions légales à l'obligation au secret du médecin, sachant que le législateur a finalement non seulement prévu des cas d' « obligation » de divulgation de données par celui-ci à des tiers mais aussi des cas de «possibilité» de communication. Le code de déontologie énumère ainsi :

a) La communication aux médecins inspecteurs du service du contrôle de l'INAMI, dans le cadre de la législation sur l'assurance maladie invalidité, des seuls renseignements nécessaires à l'exercice de leur mission de contrôle dans les limites strictes de celle-ci. La communication de ces renseignements et leur utilisation par les médecins inspecteurs sont subordonnées au respect du secret professionnel.

b) La communication de données ou des renseignements médicaux relatifs à l'assuré aux médecins-conseils des organismes assureurs en matière d'assurance maladie-invalidité et dans les limites de la consultation médico-sociale. Le médecin-conseil d'un organisme assureur est, comme tout médecin, tenu de respecter le secret professionnel; il ne doit donner à cet organisme que ses conclusions administratives.

c) La déclaration aux inspecteurs d'hygiène des maladies transmissibles épidémiques, suivant les modalités et conditions prévues par la législation en la matière.

d) L'envoi, à l'inspecteur d'hygiène, de rapports concernant les maladies vénériennes en application de la législation relative à la prophylaxie de ces maladies.

e) Les communications et les déclarations à l'officier de l'état civil en matière de naissance conformément aux dispositions légales.

f) La délivrance, en vue de permettre les déclarations d'accidents de travail, de certificats médicaux réglementaires et contenant toutes les indications en rapport direct avec le traumatisme causal.

g) La délivrance de rapports et certificats médicaux en exécution des prescriptions légales relatives à la protection de la personne des malades mentaux et à la protection des biens des personnes totalement ou partiellement incapables d'en assumer la gestion en raison de leur état physique ou mental.

h) La délivrance de rapports médicaux en exécution des prescriptions légales relatives aux maladies professionnelles.

i) La délivrance de certificats médicaux en exécution des prescriptions légales relatives aux contrats d'assurance terrestre.

Il existe encore d'autres exceptions à la règle du secret du soignant telles que les dispositions légales particulières relatives à la maltraitance des enfants (art. 458 bis du Code pénal) et les situations exceptionnelles d'état de nécessité, lorsqu'un péril grave et imminent peut justifier la révélation du secret.

Le secret médical partagé constitue une autre hypothèse de dérogation à la règle du secret, à envisager lors du traitement informatisé de données du patient au sein d'un service des urgences hospitalier. Cette théorie permet la communication d'informations entre les praticiens soignant un même patient et ce, moyennant le

respect des conditions suivantes : la communication de renseignements par un praticien professionnel ne peut se faire que dans l'intérêt du patient, à l'égard d'un autre praticien tenu au secret et chargé de poursuivre l'élaboration du diagnostic ou des soins du patient; la communication doit être limitée aux données utiles et nécessaires à la mission (du moment) du destinataire des données. Cette divulgation ne peut se faire que si le patient ne s'y oppose pas (ce qui implique qu'il en soit informé).

Ces conditions doivent s'exprimer au travers de mesures techniques et organisationnelles adéquates.

I.2.2 Détermination des types de données à traiter et des catégories de destinataires des données

La loi "vie privée" précise que, pour les personnes agissant sous l'autorité du responsable du traitement, l'accès aux données ainsi que les possibilités de traitement doivent être limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les besoins du service (article 16, §2, 2°, de la loi "vie privée").

Le responsable du traitement doit d'ailleurs désigner les catégories de personnes ayant accès aux données à caractère personnel relatives à la santé avec une description précise de leur(s) fonction(s) par rapport au traitement des données visées (art. 25 de l'arrêté royal du 13 février 2001). La liste de ces catégories de personnes doit être tenue à la disposition de la Commission de protection de la vie privée.

Le responsable du traitement des données du patient doit donc déterminer les catégories de personnes susceptibles de traiter les données du patient et les catégories de données auxquelles chaque utilisateur aura accès en fonction de ses spécialités et compétences.

Ces règles correspondent aux conditions de la théorie du secret partagé dans la mesure où, seules, les données (du patient) utiles et nécessaires à la mission d'un praticien peuvent lui être communiquées.

En pratique, la gestion de l'accès aux données relatives à la santé du patient en fonction de la spécialité et de l'identité du praticien soignant n'est pas évidente. Elle l'est encore moins dans un service des urgences où l'on pourrait considérer que chaque praticien soignant a besoin d'avoir accès à toutes les données disponibles à propos du patient. Le débat doit intervenir à ce sujet au sein de l'hôpital et du service. Le responsable du traitement devra in fine répondre à la question : à quelles données auront accès les médecins de telle spécialité, leurs stagiaires, les infirmières ... ?

En tout cas, la règle de base est la séparation des données du patient en fonction de leur nature. Ainsi, toutes les données à caractère personnel relatives à la santé du patient ne peuvent pas être accessibles aux collaborateurs des praticiens qui ne participent pas aux soins prodigués au patient concerné (ex : secrétaires, service comptable, service social, service d'accueil, ...).

A cet égard, le Conseil de l'Europe recommande en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, que le traitement des données médicales soit en règle générale conçu de façon à permettre la séparation (art. 9.2., e, de la recommandation R(97) 5 du 13 février 1997 relative à la protection des données médicales) :

- des identifiants et des données relatives à l'identité des personnes,
- des données administratives,
- des données médicales,
- des données sociales,
- des données génétiques.

Par ailleurs, en vertu de la loi sur les droits du patient, ce dernier dispose d'un droit de consultation direct de son dossier médical, à l'exception des données relatives aux tiers et des annotations personnelles des praticiens. Quant aux données relevant du privilège thérapeutique (données sensibles que le praticien estime ne pouvoir être consultées par le patient que de manière indirecte), elles ne pourront être consultées que par l'intermédiaire d'un praticien professionnel désigné par le patient. En cas de consultation par la personne de confiance désignée par le patient ou par le praticien

professionnel désigné par le patient en cas d'exercice du privilège thérapeutique, cet intermédiaire peut consulter les annotations personnelles du praticien. Il est donc opportun de catégoriser les données du patient pour permettre un accès sélectif en fonction des droits de la personne qui les consulte.

I.2.3 Fixation de la procédure d'information du patient sur le traitement de ses données

Le responsable du traitement est tenu de veiller à ce que le patient soit informé de l'existence du traitement des données qui le concernent et de ses diverses modalités (art. 9 de la loi "vie privée").

Cette obligation est fondamentale. Elle constitue la pierre angulaire de la loi "vie privée" en traduisant les principe de transparence et de loyauté qu'elle entend mettre en œuvre. Le responsable du traitement peut confier cette tâche d'information à la personne en contact avec le patient ou amenée à récolter les données auprès de celui-ci.

Si la loi "vie privée" mentionne déjà les informations à communiquer au patient (article 9 et article 25 à 27 de son arrêté royal d'exécution du 13 février 2001), l'arrêté royal du 23 octobre 1964, portant fixation des normes auxquelles les hôpitaux doivent répondre, précise différents éléments à porter à la connaissance du patient :

1. Les finalités du traitement des données à caractère personnel.
2. L'identité et les coordonnées du responsable du traitement et de la personne qui peut agir en son nom.
3. La base légale ou réglementaire qui autorise le traitement des données.
4. Le nom du médecin qui exerce la responsabilité et la surveillance du traitement des données (désigné par le responsable du traitement).
5. Le nom du conseiller en sécurité chargé de la sécurité de l'information.
6. Les catégories de personnes dont les données font l'objet d'un traitement.
7. La nature des données traitées et la manière dont elles sont obtenues.
8. L'organisation du circuit des données médicales à traiter.
9. La procédure suivant laquelle, si nécessaire, les données sont rendues anonymes.
10. Les procédures de sauvegarde afin d'empêcher la destruction accidentelle ou

illicite de données, la perte accidentelle de données ou l'accès illicite à celles-ci, leur modification ou diffusion illicite.

11. Le délai au-delà duquel les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées.
12. Les rapprochements, interconnexions ou toute forme de mise en relation de données faisant l'objet du traitement.
13. Les interconnexions et les consultations.
14. Les cas où les données sont effacées.
15. La manière dont les patients peuvent exercer leurs droits visés dans la loi "vie privée" du 8 décembre 1992.

Au sein d'un hôpital, l'information du patient s'effectue en principe par la remise d'office d'un exemplaire du règlement relatif à la protection de la vie privée.

Le responsable du traitement pourrait néanmoins imaginer une manière plus efficace et plus pédagogique d'informer les patients à cet égard.

Par ailleurs, les informations dues au patient doivent lui être fournies au plus tard au moment où les données sont récoltées auprès de lui, ou, si celles-ci ont été récoltées auprès de tierces personnes, au moment de leur enregistrement ou de leur première communication à un tiers.

Dans un contexte d'urgence, les règles décrites ci-dessus peuvent être nuancées. Face à un patient inconscient ou lorsque son état nécessite une intervention urgente, l'information peut être postposée jusqu'à ce que le patient soit en état de la recevoir.

Entre-temps, l'information sur le traitement des données doit-elle ou peut-elle être communiquée au « représentant » du patient tel que prévu dans la loi relative aux droits du patient ? Si la réponse est positive en ce qui concerne les représentants des enfants pris en charge, elle est moins certaine pour les mineurs adolescents ou les adultes incapables de fait. Une réponse positive ne serait toutefois pas illogique dans la mesure où le représentant du patient se voit reconnaître de larges pouvoirs tels que, dans une certaine mesure, la consultation de leur dossier (articles 12 à 15). Il n'est dès lors pas inadéquat d'informer ces représentants du patient sur le

« traitement » informatisé des données le concernant.

S'agissant en outre de la théorie du secret médical partagé, le patient doit aussi être informé des « communications » de données qui le concernent d'un professionnel à un autre, pour pouvoir éventuellement s'y opposer. Le responsable du traitement doit dès lors informer le patient des transferts de données entre professionnels.

I.2.4 Mesures d'information à l'égard des utilisateurs à propos de la collecte de données, de leur pertinence, de leur exactitude, et de la limitation de leur conservation dans le temps

Les données relatives à la santé doivent être collectées auprès de la personne concernée, sauf exceptions (cf. *infra*).

Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues. Les données doivent être exactes et, si nécessaire, mises à jour . Enfin, les données doivent être conservée pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues.
Il appartient au responsable du traitement d'avertir et d'informer les utilisateurs du traitement sur ces mesures, de manière à ce que ces derniers, seuls susceptibles de traiter et accéder aux données du patient à raison de la règle du secret médical, puissent les appliquer correctement.

I.2.5 Fixation de la politique à mener en matière de confidentialité et de sécurité

Le responsable du traitement doit prendre toutes les mesures nécessaires pour garantir la confidentialité et la sécurité des données à caractère personnel. Celles-ci seront assurées par des obligations de secret et de confidentialité, d'une part, et par l'adoption de mesures techniques et organisationnelles, d'autre part.

a. Les obligations au secret et à la confidentialité

La règle du secret médical participe certainement à la confidentialité du traitement.

La loi "vie privée" prévoit en outre que le professionnel des soins de santé sous la

responsabilité duquel est effectué le traitement de données à caractère personnel relatives à la santé du patient, est soumis au secret, de même que ses préposés ou mandataires (art 7, § 4, al. 3, de la loi "vie privée").

Lors du traitement des données relatives à la santé du patient, le responsable du traitement doit veiller à ce que toutes les personnes, lui compris, qui ont accès aux données soient tenues au respect de leur caractère confidentiel, que ce soit par ou en vertu d'une obligation légale, statutaire ou par une disposition contractuelle équivalente (art. 25, 3°, de l'arrêté royal du 13 février 2001).

Si le responsable du traitement n'est pas un praticien en charge du patient, il ne peut pas avoir accès aux données du patient protégées par le secret médical. La même règle s'applique aux personnes qui ne participent pas aux soins, sauf si ces personnes peuvent être reconnues en tant que collaborateurs obligés du personnel soignant (ex. les secrétaires, les informaticiens dans certaines hypothèses, etc.).

b. Les mesures techniques et organisationnelles

Tant la protection de la vie privée que le respect du secret médical imposent l'adoption de mesures techniques et organisationnelles destinées à assurer la sécurité du traitement des données du patient.

Concrètement, le responsable du traitement doit prendre toutes les mesures techniques et organisationnelles nécessaires afin de protéger les données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle, ainsi que contre la modification, l'accès et tout autre traitement non autorisé des données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat (art. 16, § 4, de la loi "vie privée").

Le niveau de protection est apprécié au regard, d'une part, de l'état de la technique et des frais qu'entraîne l'application de ces mesures, et d'autre part, de la nature des données à protéger des risques potentiels. Les données médicales étant des données sensibles, le niveau de protection doit être maximal.

Le Conseil de l'Europe recommande aussi de prendre des mesures appropriées pour

assurer la confidentialité, l'intégrité et l'exactitude des données traitées (Rec. n° R(97) 5, o.c., art. 9.2), ces mesures devant viser :

a) à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations);

b) à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données);

c) à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire);

d) à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);

e) en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation :
   - des identifiants et des données relatives à l'identité des personnes;
   - des données administratives;
   - des données médicales;
   - des données sociales;
   - des données génétiques (contrôle d'accès);

f) à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication);

g) à garantir qu'il puisse être vérifié et constaté a posteriori qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction);

h) à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

i) à sauvegarder les données par la constitution de copies de sécurité (contrôle de

disponibilité).

Le Conseil national de l'Ordre des Médecins a rendu divers avis en matière de sécurité des traitements de données à caractère personnel relatives à la santé dans un contexte thérapeutique[3] .

Concrètement, plusieurs mesures de base doivent retenir l'attention.

(1) Les règles d'identification des utilisateurs doivent être fixées (par exemple, insertion d'une carte professionnelle, mot de passe, empreinte digitale, etc.). Le mode d'identification doit être strictement personnel à chaque utilisateur.

(2) Les identifiants et les données relatives à l'identité des personnes doivent être séparés des données administratives, des données médicales, des données sociales, et des données génétiques en précisant qui est susceptible d'accéder à chacune de ces catégories de données.

(3) La possibilité d'accès aux données doit être limitée dans le temps en fonction des missions des utilisateurs. A cet égard, il importe de déterminer les garanties permettant de s'assurer que le praticien qui traite les données relatives à la santé est effectivement en charge du patient ou, tout au moins, qu'il est attaché au service en charge du patient.

(4) L'installation d'un détecteur de virus, d'un système de sauvegarde automatique ; le dédoublement des bases de données, la conservation du matériel informatique dans un lieu sûr, le respect des normes de chiffrement en cas de communication des données sur des réseaux en intra et extra-hospitalier.

(5) La disponibilité des données, leur intégrité et leur imputabilité à un praticien

[3] www.ordomedic.be : Communications électroniques - secret médical », 22 avril 1995 ; « Télématique médicale », 15 février 1997 ; « Dossier médical global informatisé », 12 décembre 1998 ; « Sécurité des données transmises par Internet », 20 février 1999 ; « Dossier médical et infirmier électronique », 17 février 1999 ; avis du 17 février 2001 relatif à la protection de la confidentialité lors de la transmission de données médicales à caractère personnel par le réseau Internet, (chiffrement et signature électronique) ; avis du 15 juin 2002 relatif à la tenue de bases de données médicales contenant des données nominatives ou identifiables.

est importante (cf. *infra*, utilisation de la signature électronique pour l'encodage de certains documents).

(6) La traçabilité des accès et des opérations effectuées sur les données du patient doit être assurée afin de permettre un contrôle a posteriori des utilisations des données.

I.2.6 Déclaration à la commission de la protection de la vie privée

Avant de mettre en œuvre un traitement de données à caractère personnel entièrement ou partiellement automatisé, le responsable du traitement doit déclarer le traitement à la Commission de la protection de la vie privée (art. 17 de la loi "vie privée").

Le formulaire de déclaration est disponible sur le site Internet de la Commission (http:/www.privacy.fgov.be). La déclaration sur support magnétique coûte 25 EUR, tandis que la version papier entraîne la perception d'une contribution de 125 EUR.

La déclaration doit reprendre les éléments suivants.

- la date de la déclaration et, le cas échéant (d'office pour les données relatives à la santé), la mention de la loi, du décret , de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé,
- les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et le cas échéant, de son représentant en Belgique,
- la dénomination du traitement automatisé,
- la finalité ou l'ensemble des finalités liées du traitement automatisé,
- les catégories de données à caractère personnel qui sont traitées (celles-ci étant des en l'occurrence des données relatives à la santé, il en faut une description précise),
- les catégories de destinataires à qui les données peuvent être fournies,
- les garanties dont doit être entourée la communication de données aux tiers,
- les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit,
- la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées,

- une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement.

La Commission peut demander les informations supplémentaires qu'elle juge pertinentes.

II. Le sous-traitant du responsable du traitement des données du patient

Le responsable du traitement peut confier à un sous-traitant tout ou partie du traitement des données à caractère personnel. Le sous-traitant est « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données » (art. 1, § 5, de la loi "vie privée").

Le sous-traitant doit répondre à un certain nombre d'exigences; à cet effet, le responsable du traitement doit (art. 16 de la loi "vie privée") :

1° choisir un sous-traitant qui apporte les garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements ;
2° veiller au respect de ces mesures, notamment par la stipulation de mentions contractuelles ;
3° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement ;
4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu ;
5° consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences de traitement sur instruction du responsable.

III. Le professionnel de la santé sous la responsabilité et la surveillance duquel le traitement de données à caractère personnel relatives à la santé doit être effectué

S'agissant spécifiquement du traitement de données relatives à la santé, leur

traitement doit se faire sous la responsabilité d'un professionnel de la santé (art. 7, § 4, al. 1, de la loi "vie privée"). Cette fonction ne se confond pas avec la notion de responsable du traitement définie à l'article 1, § 4, de la loi "vie privée". Néanmoins, le responsable du traitement peut remplir cette fonction s'il est un professionnel de la santé.

En outre, dans le cadre d'un traitement de données relatives à la santé à finalité thérapeutique, le traitement doit se faire sous la surveillance d'un professionnel des soins de santé (art. 7, § 2, j, de la loi "vie privée"). On considère généralement que les fonctions de responsabilité et de surveillance du traitement de données à caractère personnel relatives à la santé se confondent et sont exercées par une même personne.

La notion de « professionnel des soins de santé» n'est toutefois pas définie dans la loi "vie privée". Elle se rapproche quand même de la notion de « praticien professionnel » visée dans la loi sur les droits du patient, à savoir le professionnel disposant du titre requis pour prodiguer des soins de santé.

Le médecin spécialisé en gestion des données de santé (spécialité reconnue par l'arrêté ministériel du 15 octobre 2001) pourrait exercer ces missions de responsabilité et surveillance du traitement des données relatives à la santé du patient.

Ceci étant, les tâches précises de la personne chargée de la responsabilité et de la surveillance du traitement des données relatives à la santé n'ont pas été définies par la loi.

IV. Le conseiller en sécurité

L'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux doivent répondre, impose au responsable du traitement de désigner un conseiller en sécurité. Celui-ci « doit veiller à la sécurité des applications et à la prise de mesures techniques et organisationnelles appropriées de manière à garantir le respect de la confidentialité des données ; il doit également veiller au contrôle des accès et

autres » (Avis n°33/2002 du 22 août 2002 de la commission de protection de la vie privée).

S'il ne peut éviter d'accéder au contenu des données relatives à la santé des patients, il devra respecter son obligation à la confidentialité telle que prévue à l'article 25, 3°, de l'arrêté royal du 13 février 2001 pris en vertu de la loi "vie privée".

V. Les utilisateurs du système d'information dans le service des urgences

Les praticiens soignant les patients en service d'urgences sont concernés par l'informatisation de leur service puisqu'ils sont les utilisateurs du système d'information.

V.1 Respect des conditions d'accès

Chaque praticien ne peut accéder au système d'information que s'il est en charge d'un patient, et si c'est utile et nécessaire aux soins qui doivent lui être prodigués, et moyennant son identification régulière.

Il s'ensuit déjà qu'un médecin-conseil d'une société d'assurance, par exemple, ne peut pas avoir accès au système d'information du service des urgences.

Par ailleurs, Il n'est en tout cas pas acceptable d'autoriser le libre accès au système d'information sans identification préalable de tout utilisateur. A cet égard, la technologie offre suffisamment de moyens d'identification rapides et ergonomiques pour satisfaire à cette exigence élémentaire.

V.2 Respect des conditions liées à la collecte des données, à la pertinence des données traitées, à leur exactitude, et à leur conservation limitée dans le temps

- Les données à caractère personnel relatives à la santé doivent être collectées auprès de la personne concernée (art. 7, § 5, de la loi "vie privée").

De manière subsidiaire, les données à caractère personnel relatives à la santé peuvent être collectées auprès d'une autre personne à condition que ce soit nécessaire aux fins du traitement de données ou que le patient ne soit pas en mesure de les fournir. Le patient doit être averti de la collecte de données auprès d'un tiers (par exemple, un proche ou un autre praticien). Il doit en être informé au

moment de l'enregistrement des données ou au moment de leur première communication à un autre tiers, avec postposition de l'information s'il n'est pas en état de recevoir l'information.

Pour rappel, le patient doit avoir été informé des transferts possible de données entre praticiens.

- Le patient a droit à ce que ses données soient « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement » (art.4, § 1, 3°, loi "vie privée").

Dans la relation thérapeutique, l'adéquation, la pertinence, l'exactitude, et le caractère non excessif des données traitées s'apprécient d'abord au regard de la finalité de soins.

L'exactitude impose que la donnée soit conforme à la réalité, complète et mise à jour si nécessaire.

Le responsable du traitement doit prendre les mesures nécessaires pour que les praticiens en charge du patient, seuls susceptibles de traiter directement les données protégées par le secret médical, mettent eux-mêmes à jour les données ou rectifient celles qui sont inexactes ou incomplètes.

Il n'est toutefois pas toujours aisé de considérer si une donnée est « exacte» ou non, plusieurs d'entre elles relevant d'appréciations subjectives, demeurant hypothétiques ou non définitives. Le diagnostic peut différer d'un médecin à l'autre, laissant place à une marge d'appréciation thérapeutique.

Par ailleurs, si l'on peut concevoir que le praticien rectifie une donnée qu'il a lui-même encodée - la trace de la première donnée encodée devant toutefois rester - , il est difficile d'imaginer que, dans le cadre d'un dossier médical « partagé », alimenté et utilisé par plusieurs praticiens d'un même service, l'un d'eux efface ou corrige purement et simplement une donnée encodée par un collègue.

Une procédure devrait être établie pour résoudre une éventuelle contestation entre plusieurs praticiens à propos d'une même donnée. A cet égard, les praticiens concernés (et éventuellement le patient) devraient pouvoir faire valoir leur point de vue. Ensuite, le résultat de la concertation devrait apparaître. En cas de correction d'une donnée antérieurement encodée, celle-ci devrait subsister en archivage et le fait de sa correction devrait apparaître et être mis en évidence à l'égard des différents utilisateurs du réseau.

- Les données ne doivent être conservées que le temps nécessaire pour réaliser la finalité poursuivie (art. 4, § 1, 5°, de loi "vie privée").

Le responsable du traitement doit veiller à ce que le médecin de référence du patient soit attentif au délai légal de conservation des données (actuellement de 30 ans, en vertu de l'article 46 du code de déontologie médicale et de l'article 1, § 3, de l'arrêté royal du 3 mai 1999 sur le dossier médical hospitalier) à partir de la cessation de la prise en charge du patient.

A l'expiration du délai de conservation du dossier du patient, celui-ci sera archivé selon les modalités fixées par le responsable du traitement, conformément aux règles légales et réglementaires applicables.

V.3 L'encodage des données du patient en fonction de la compétence

L'encodage des données du patient doit être effectué par une personne possédant la compétence requise pour poser l'acte médical ou infirmier auquel il se rattache.

A cet égard, de nombreux praticiens gravitent au sein ou autour du service d'urgences: le médecin urgentiste, l'anesthésiste, l'infirmier, le radiologue, les praticiens du laboratoire de biologie clinique, ...

En principe, chaque praticien encode les données résultant des actes qu'il a accomplis.

Plusieurs arrêtés royaux déterminent les actes qu'un praticien, en fonction de sa qualité et de sa spécialisation, peut poser.

Conformément à l'arrêté royal n°78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé, les conditions liées au diplôme donnant droit au titre de praticien professionnel de la santé ou à la qualification de professionnel stagiaire doivent être réunies pour traiter les données à caractère personnel relatives à la santé du patient à des fins thérapeutiques, sous réserve de l'intervention d'un collaborateur ou d'une éventuelle délégation de tâches.

A titre d'exemples, le praticien encode les données relevant des missions qu'il peut accomplir légalement ; une infirmière ne peut encoder des données relatives au diagnostic que le chirurgien a posé, l'élaboration d'un diagnostic chirurgical n'entrant pas dans son champ de compétences. L'infirmière encode les données relatives aux actes déterminés à l'article 21 quinquies de l'arrêté royal n°78 du 10 novembre 1967 et précisés dans l'arrêté royal du 18 juin 1990 récemment modifié et portant fixation de la liste des prestations techniques de soins infirmiers et de la liste des actes pouvant être confiés par un médecin à des praticiens de l'art infirmier, ainsi que des modalités d'exécution relatives à ces prestations et à ces actes et des conditions de qualification auxquelles les praticiens de l'art infirmier doivent répondre.

De même, si un pharmacien hospitalier encode des données dans le système d'information du service des urgences, il doit respecter l'article 4 de l'arrêté royal n°78 du 10 novembre 1967 précisant les tâches qui lui sont confiées, ainsi que l'arrêté royal du 4 mars 1991 fixant les normes auxquelles une officine hospitalière doit satisfaire pour être agréée.

Cette exigence du respect des compétences de chaque utilisateur est importante au regard de la responsabilité de chacun. En effet, chaque praticien est responsable des données qu'il encode. Dans un avis du 15 juin 2002, le Conseil national de l'Ordre des médecins signale que « (...) *l'enregistrement par le médecin de données personnelles médicales dans une base de données engage le responsabilité du médecin qui a la charge du patient (...)* ».

Ceci étant, l'encodage ne relève pas directement de l'art de guérir au sens strict. Il n'est donc pas exclu que le praticien (notamment en situation d'urgence) confie à un tiers la charge de l'encodage des données relatives aux actes qu'il a lui-même posés.

Le Conseil National de l'Ordre des Médecins précise à ce propos que « (...) Le médecin en charge d'un dossier médical peut confier, sous sa responsabilité, certaines tâches administratives nécessitant pour les réaliser la connaissance d'une partie des éléments du dossier médical, à des collaborateurs non-médecins (...) » (avis du 16 juillet 2002).

Dans l'hypothèse de la délégation de tâches administratives (dont l'encodage), le praticien doit suivre plusieurs mesures de précaution. En effet, le fait qu'un tiers procède à l'enregistrement des données n'enlève rien à la responsabilité du praticien.

Ainsi, le praticien doit s'être identifié de manière à ce que l'on sache qu'il est le responsable des données encodées par le tiers (à moins que le tiers n'ait un code d'accès spécial lui permettant d'encoder des données au nom d'un praticien identifié). Le praticien doit prêter attention au respect du secret médical dans le choix du tiers encodeur (il doit s'agir d'un collaborateur obligé) et éviter de confier cette tâche à une personne non tenue au secret médical et extérieure à l'offre des soins. Enfin, il doit vérifier les données encodées et les valider.

Certains actes nécessitent la signature d'un médecin (cf. l'arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987 doit répondre, art. 2, § 2). Le recours à la signature électronique peut dès lors s'avérer utile.

V.4 Le respect du principe du secret médical partagé

Le praticien ne doit accéder qu'aux données nécessaires et utiles à la réalisation de sa mission thérapeutique.

Dans la mesure du possible, le praticien dialoguera avec le patient à propos du traitement des données et l'informera des opérations qu'il effectue, surtout lorsqu'il est amené à encoder des données particulièrement sensibles et potentiellement accessibles à d'autres professionnels du service.

VI. Le patient

Le patient est bien entendu concerné par le système d'information du service des urgences. En effet, ce sont les données relatives à sa propre santé qui feront l'essentiel de l'objet de l'informatisation. Le patient peut jouer un rôle important, d'une part par la revendication de certains droits à l'égard du traitement informatisé de ses données, et d'autre part, par les informations qu'il confiera au praticien lors de l'anamnèse.

VI.1 Que peut exiger le patient ?

VI.1.1 Le droit de consulter son dossier médical et d'en obtenir une copie

- Le patient a le droit de consulter lui-même son dossier médical (art. 9, § 2, de la loi relative aux droits des patients). S'il le souhaite, le patient peut se faire assister par une personne de confiance qu'il aura désignée. Il peut aussi exercer ce droit par l'entremise de cette même personne. Ce droit de consultation n'est pas absolu ; les annotations personnelles du praticien, ainsi que les données concernant les tiers, en sont en effet exclues. La personne de confiance a toutefois accès aux annotations personnelles du praticien.

Une autre exception propre au droit médical vient aussi limiter la portée de ce droit de consultation : l'exception thérapeutique (art. 33 du code de déontologie médicale) consacrée par l'article 7, § 4, de la loi relative aux droits du patient. Dans l'hypothèse où le praticien estime que des données sont particulièrement sensibles et que leur consultation directe par le patient risque de lui porter préjudice, le patient ne pourra pas consulter lui-même son dossier, mais il devra désigner un praticien professionnel pour exercer son droit. Celui-ci aura accès aux annotations personnelles du praticien.

Il faut bien entendu tenir compte de ces modalités du droit à la consultation lors de l'informatisation du service des urgences.

Le patient a également le droit d'obtenir, au prix coûtant, une copie de son dossier ou une partie de celui-ci, à moins que le praticien dispose d'indications claires selon lesquelles le patient subit des pressions afin de communiquer son dossier à des tiers

(article 9, § 3, de la loi relative aux droits du patient).

- En pratique, à qui va s'adresser le patient pour exercer son droit de consultation?

Au regard de la loi "vie privée", le patient doit s'adresser au responsable du traitement. Mais, à raison du secret médical, celui-ci ne peut statuer sur la requête du patient que s'il est son médecin. A défaut, le responsable du traitement doit répercuter la requête du patient à la personne habilitée pour y répondre.

Dans un hôpital, il semble opportun à cet égard que le patient désigne un médecin de référence qui participe aux soins de santé qui lui sont prodigués et qui sera la personne habilitée à répondre à sa requête, en suite de la demande formulée au responsable du traitement.

C'est aussi ce médecin de référence qui pourrait décider doit refuser une copie du dossier en présence de pressions de tiers.

Le patient devrait avoir le droit de demander la liste des personnes qui ont accédé à ses données (contrôle *a posteriori* des flux des données au sein du service ou de l'hôpital).

VI.1.2 Le droit d'opposition au traitement des données

Le patient a le droit de s'opposer à ce que ses données à caractère personnel le concernant fassent l'objet d'un traitement au sens de la loi "vie privée".

Ce droit d'opposition se justifie au nom du droit à l'autodétermination informationnelle de tout individu et s'exprime au moins de deux façons différentes.

D'une part, la loi "vie privée" prévoit que le patient peut se prévaloir de raisons sérieuses et légitimes tenant à une situation particulière pour s'opposer au traitement de ses données (art. 12, § 1, al.2).

D'autre part, la théorie du secret médical partagé implique que le patient puisse s'opposer à tout moment à ce qu'une donnée - même exacte ou pertinente -, soit

communiquée d'un professionnel des soins de santé à l'autre et ce, même sans raison légitime et sérieuse. Pour rappel, cela implique que le patient doit être préalablement informé de toute communication entre les professionnels ou, à tout le moins, des modalités de fonctionnement du réseau impliquant des transferts « potentiels » de données entre ces professionnels.

Si le patient s'oppose à ce qu'une ou plusieurs données soient communiquées à différents professionnels, la qualité du système informatique risque de s'en ressentir. Comment veiller alors à la qualité de l'information disponible ? Le praticien doit avertir le patient des risques liés à la non-communication de l'information. Dans le cas d'une opposition du patient, le médecin devrait indiquer que l'information disponible est incomplète.

Le patient devrait pouvoir, s'il a des souhaits particuliers quant à la (non) informatisation de certaines données, demander que ces instructions soient accessibles à tous les utilisateurs du réseau.

VI.1.3 Le droit de rectification, de suppression et d'interdiction d'utilisation de certaines données

- Le patient a le droit d'obtenir, sans frais, la rectification de toute donnée à caractère personnel inexacte qui le concerne. Le patient adresse une requête en ce sens au responsable du traitement (art. 12, § 1, al. 1 de la loi "vie privée").

L'application de ce droit aux données à caractère personnel relatives à la santé est délicate. Quand peut-on affirmer l'inexactitude d'une donnée médicale parfois empreinte de subjectivité et d'appréciations hypothétiques ?

Indépendamment de ce problème d'interprétation et d'appréciation, le responsable du traitement ne peut de toute façon pas intervenir lui-même sauf s'il est en charge du patient. Il doit dès lors répercuter la requête au praticien responsable de la donnée et donc habilité à procéder à la rectification.

Le droit du patient d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel qui le concerne et qui, compte tenu de la

finalité du traitement poursuivie, est incomplète ou non pertinente, ou dont l'enregistrement, la communication sont interdits ou encore qui a été conservée au-delà de la période autorisée (art. 12, § 1, al. 5 de la loi "vie privée").

Pour rappel, le patient a le droit de demander la suppression d'une donnée encodée destinée à être « communiquée » même si la donnée est exacte, complète et pertinente. Ici encore, le patient s'adressera au responsable du traitement qui répercutera la requête au praticien qui a encodé la donnée litigieuse.

Que ce soit dans le cadre d'une demande de rectification ou de suppression d'une donnée, le praticien et le patient devraient à tout le moins avoir eu un entretien et pu dialoguer sur la contestation. Pour le cas où le praticien signalerait au responsable du traitement que, selon lui, la donnée ne peut être corrigée ou supprimée, le patient peut s'adresser à la Commission de la protection de la vie privée ou au président du tribunal de première instance de son domicile siégeant en référé.

Une médiation, telle que prévue par la loi relative aux droits du patient, entre le praticien qui a encodé la données et le patient pourrait aussi s'avérer opportune.

VI.1.4 Le droit de porter plainte

En cas de non respect de ses droits, le patient peut porter plainte. Différentes possibilités de recours sont offertes au patient, en fonction de la loi et des droits en cause.

En application de la loi "vie privée", le patient peut se plaindre auprès du responsable du traitement. Il peut aussi adresser une plainte auprès du président du tribunal de première instance de son domicile siégeant comme en référé ou adresser une plainte auprès de la Commission de protection de la vie privée, dans la mesure où cette plainte a trait à sa mission de protection de la vie privée. Dans ce dernier cas, après l'examen de la recevabilité de la demande de la personne concernée, la Commission peut accomplir toute mission de médiation qu'elle juge utile.

Le patient peut également déposer plainte au pénal, dès lors que des violations des dispositions de la loi du 8 décembre 1992 érigées en infraction ont été commises ou que d'autres infractions sont en cause.

Le patient peut aussi introduire une action en responsabilité civile s'il a subi un dommage suite au comportement litigieux en cause.

En vertu de la loi sur les droits du patient, ce dernier peut saisir la fonction de médiation de l'hôpital compétente pour toute plainte concernant l'exercice des droits qui lui sont reconnus en vertu de ladite loi, en ce compris le droit à la protection de la vie privée.

VI.1.5 Le droit à la réparation du préjudice

En vertu de la loi "vie privée", le patient a le droit de demander au responsable du traitement la réparation du dommage causé par un acte contraire aux dispositions déterminées par la loi "vie privée". (art. 15bis de la loi "vie privée")

Le patient ne doit pas rapporter la preuve de la faute du responsable ; il appartient à ce dernier de prouver que le fait générateur du dommage ne lui est pas imputable pour être exonéré de toute responsabilité.

VI.2 L'obligation de loyauté du patient ?

En vue du bon fonctionnement du système d'information et de l'octroi efficient de soins de santé, le patient devrait fournir des informations exactes et pertinentes. Il existe cependant des situations où l'opposition du patient de voir des informations trop sensibles être reprises dans le système d'information devrait être respectée.

A tout le moins, le patient doit connaître la conséquence de son opposition au traitement de ses données sur le fonctionnement du système d'information et donc plus fondamentalement sur les risques potentiels sur la qualité des soins qui lui seront prodigués.

Ceci étant, le patient est plus à même de confier des informations complètes et correctes lorsqu'un climat de confiance optimal s'est instauré entre les protagonistes, étant entendu que certaines exigences légales ou réglementaires peuvent miner

totalement ou partiellement cette relation de confiance. Il appartient à cet égard à l'Etat de prendre ses responsabilités en terme de Santé Publique.