ORDRE NATIONAL DES MÉDECINS
Conseil National de l'Ordre

Dématérialisation des documents médicaux
Créer la confiance pour favoriser l'informatisation

I : les dossiers médicaux et les correspondances

Rapport adopté par le Conseil national de l'Ordre des médecins
le 18 juin 2010

Rapporteur : Docteur Jacques Lucas.

Nous remercions :
Pour leurs contributions juridiques, Mesdames J.COAT, C.HERON, M.THUBEUF et Monsieur A.TORNAY,
Madame Sylvie BRETON, conseiller juridique, et les membres de la section Ethique et déontologie du Conseil national,
Monsieur M. FRANC, président de section honoraire au Conseil d'Etat, président de la Chambre disciplinaire nationale d'appel
Monsieur Paul COURBIS, DIS du CNOM pour sa lecture technique,
Madame Dominique Lehalle pour sa relecture externe

Les technologies de l'information et de la communication font désormais partie intégrante de l'environnement professionnel des médecins. Elles offrent des possibilités d'exploitation des données et des connaissances difficilement imaginables il y a 15 ans à peine. En favorisant l'échange et le partage de documents médicaux, elles jouent un rôle important dans la coordination des soins. Elles contribuent, de façon générale, à l'amélioration de la qualité des soins en facilitant l'accès, sans perte de temps, aux données nécessaires à la prise de décision et à la continuité de la prise en charge. L'informatisation de la pratique médicale apporte, enfin, les moyens de dégager du temps pour l'écoute et les soins aux patients.

Les transformations induites par l'avènement du numérique dans la santé doivent cependant s'accomplir dans un cadre de confiance renouvelé et adapté. Le Conseil National de l'Ordre des Médecins s'y implique activement.

Ainsi, cette publication complète les deux livres blancs déjà diffusés par l'Ordre :

- sur l'informatisation de la santé, en mai 2008,
- sur la télémédecine, en janvier 2009.

Par son engagement dans la construction du système d'information de santé, le CNOM poursuit un double objectif : accélérer l'usage des technologies de l'information et de la communication pour améliorer la qualité des soins et contribuer à garantir les fondements de la confiance des médecins et des patients dans le nouvel espace numérique de santé.

En passant à l'ère de la dématérialisation, les médecins se retrouvent confrontés à des questions pratiques nouvelles sur les plans déontologique et réglementaire. C'est pourquoi le CNOM a souhaité, en publiant ce rapport, rappeler et synthétiser les principes et recommandations qui répondent aux exigences déontologiques de leur exercice.

Bien que les exercices professionnels soient divers, tant dans les secteurs de soins que dans les autres secteurs d'activités médicales, le CNOM rappelle que tous les médecins sont soumis aux mêmes règles de déontologie professionnelle qui s'attachent ici principalement à la protection et la préservation de la confidentialité des données personnelles de santé. C'est, avec la reconnaissance confirmée de leurs compétences, le socle de la confiance massive dont les médecins disposent près des patients.

Les recommandations du CNOM

Nous avons inclus dans le corps du rapport qui suit des encadrés de recommandations. Elles ont des destinataires variés … et souvent associés. Nous souhaitons cependant mettre en exergue quelques-unes d'entre elles.

Le CNOM recommande :

- que le médecin et/ou l'établissement, le réseau de santé, les différentes structures médicales s'assurent que **le patient est informé que ses données de santé font l'objet d'un traitement informatisé**, qu'il puisse exercer son droit d'opposition, et que son consentement a été recueilli dans tous les cas où il est exigé ;

- que les médecins appelés à échanger ou à partager des données de santé dans le parcours de soins d'un patient par l'utilisation des technologies de l'information et de la communication **soient identifiés et authentifiés de façon personnelle** dans l'espace informatique ;

- que les accès des médecins aux documents médicaux dématérialisés soient régis par des **règles d'habilitation claires et que leurs connexions soient tracées** ;

- que la conservation des documents numériques soit réalisée dans des conditions propres à **identifier leurs auteurs et à garantir leur intégrité, ainsi que leur exploitabilité dans le temps** ;

- **que les dispositions réglementaires relatives à la sécurité et les référentiels de chiffrement qui seront adoptés soient adaptés à la préservation de la confidentialité ainsi qu'aux usages professionnels, en concertation avec tous les acteurs concernés, afin d'être rapidement mises en œuvre** ;

- **que les systèmes soient interopérables**, suivant en cela les déclarations de la Commission européenne aux Etats membres, notamment pour assurer le déploiement des applications de télémédecine ;

- que la mise à disposition des **télé-services, notamment ceux de l'Assurance-maladie, allège réellement les tâches administratives**. Cela impose une concertation urgente autour du poste de travail du professionnel de santé à laquelle le CNOM doit être associé ;

- que les applications informatiques et systèmes d'information utilisés par les médecins du travail, médecins scolaires, médecins-conseils, médecins experts, médecins d'assurance respectent **les conditions générales de confidentialité et de sécurité qui s'imposent dans l'espace numérique de santé, et qui s'imposent aussi de par la loi**.

Sommaire

Le dossier médical : contenu et conservation

L'accès au dossier médical

Les échanges par voie électronique

Un titre second suivra ce titre premier et s'appliquera à la dématérialisation des données personnelles de santé dans la pratique de la Télémédecine et les applications de télésanté.

Le dossier médical : contenu et conservation

I. Les règles communes au dossier médical « papier » et au dossier médical informatisé

Le dossier médical professionnel établi pour chaque patient permet de :

- colliger les données du patient,
- assurer la continuité de la prise en charge,
- gagner du temps en organisant les informations pour retrouver rapidement les données pertinentes au moment nécessaire,
- éviter les examens redondants et les traitements inutiles,
- communiquer, si nécessaire, des éléments d'information utiles aux confrères consultés par un patient, ainsi qu'aux autres professionnels de santé le cas échéant,
- organiser la planification de la surveillance des pathologies chroniques et des actions de prévention et de dépistage,
- aider à la prise de décision,
- faciliter l'évaluation des pratiques professionnelles, par la profession elle-même.

Le CNOM recommande de ne faire figurer dans ce dossier professionnel, quelle que soit la nature de l'exercice du médecin qui le constitue, que les éléments objectifs et les interprétations consignées au cours de la démarche diagnostique. Il est déconseillé d'associer des notes personnelles du médecin, sans rapport avec les épisodes de soins ou des informations concernant des tiers, ou recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique.

A. <u>Le contenu du dossier médical</u>

1. En établissement de santé

- Le dossier médical est constitué des informations médicales propres au patient (énumérées à l'article R.1112-2 du Code de la santé publique) : *« Un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé.* Ce dossier contient au moins les éléments suivants, ainsi classés :

1.1. Les informations formalisées recueillies lors des consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier et notamment :

☛ la lettre du médecin qui est à l'origine de la consultation ou de l'admission,

☛ les motifs d'hospitalisation,

- la recherche d'antécédents et de facteurs de risques,
- les conclusions de l'évaluation clinique initiale,
- le type de prise en charge prévu et les prescriptions effectuées à l'entrée,
- la nature des soins dispensés et les prescriptions établies lors de la consultation externe ou du passage aux urgences,
- les informations relatives à la prise en charge en cours d'hospitalisation : état clinique, soins reçus, examens para cliniques, notamment d'imagerie,
- les informations sur la démarche médicale,
- le dossier d'anesthésie,
- le compte-rendu opératoire ou d'accouchement,
- le consentement écrit du patient pour les situations où ce consentement est requis sous cette forme par voie légale ou réglementaire,
- la mention des actes transfusionnels pratiqués sur le patient et, le cas échéant, copie de la fiche d'incident transfusionnel,
- les éléments relatifs à la prescription médicale, à son exécution et aux examens complémentaires,
- le dossier de soins infirmiers ou, à défaut, les informations relatives aux soins infirmiers,
- les informations relatives aux soins dispensés par les autres professionnels de santé,
- les correspondances échangées entre professionnels de santé,
- les directives anticipées,

1.2. Les informations formalisées établies à la fin du séjour. Elles comportent notamment :

a) le compte-rendu d'hospitalisation et la lettre rédigée à l'occasion de la sortie
b) la prescription de sortie et les doubles d'ordonnance de sortie
c) les modalités de sortie
d) la fiche de liaison infirmière.

1.3. Les informations recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers » (Ces informations ne sont pas communicables).

- **Le dispositif de certification** des établissements de santé porte, entre autres, sur la Gestion des données du patient. Elle fait l'objet d'une référence (N°14) parmi 28. La version 2010 du manuel de certification expose en effet les **Pratiques Exigibles Prioritaires** relatives au dossier du patient : « Outil de partage des informations, il est un élément clé de la qualité et de la continuité des soins dans le cadre d'une prise en charge pluri professionnelle et pluridisciplinaire ». (…) « L'indicateur HAS Tenue du dossier du patient évalue la traçabilité dans le dossier des éléments relatifs à l'admission, au séjour et à la sortie du patient. »

Le manuel cadre également la démarche d'amélioration attendue en trois étapes : E1 : prévoir, E2 : mettre en œuvre, E3 : évaluer/améliorer.

Ces étapes sont définies de la façon suivante :

E1 : Les règles de tenue du dossier sont formalisées et diffusées. Les règles d'accès au dossier, comprenant les données issues de consultations ou hospitalisations antérieures, par les professionnels habilités sont formalisées et diffusées.

E2 : Les éléments constitutifs des étapes de la prise en charge du patient sont tracés en temps utile dans le dossier du patient. La communication du dossier entre les professionnels de l'établissement et avec les correspondants externes est assurée en temps utile.

E3 : L'évaluation de la gestion du dossier du patient est réalisée, notamment sur la base d'indicateurs. Les résultats des évaluations conduisent aux améliorations nécessaires.

2. En cabinet libéral

- L'article R 4127-45 du Code de la santé publique (Article 45 du Code de déontologie médicale), établit que « Indépendamment du dossier de suivi médical prévu par la loi [DMP, Ndlr] *le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques.* »

- Le contenu du dossier ainsi constitué sera identique, qu'il soit conservé sous une forme « papier » ou qu'il soit informatisé.

Le CNOM recommande que la composition de cette « fiche » s'inspire des dispositions relatives au dossier tenu dans les établissements (cf supra) et déconseille des annotations sans rapport avec l'épisode de soins ou impliquant des tiers. **Le statut confidentiel de cette « fiche » impose au médecin de prendre les dispositions nécessaires pour qu'elle soit à l'abri de toute effraction**.

3. En réseau

De par leur vocation à organiser coordination et continuité des prises en charge, les réseaux de santé mettent en œuvre des carnets de suivi ou, de plus en plus fréquemment, des dossiers partagés et faisant l'objet de bases de données informatisées communes. Si la composition de ces dossiers comporte des données similaires aux informations décrites ci-dessus (antécédents, comptes-rendus, prescriptions, etc.), s'y ajoutent également des données de suivi et d'alertes spécifiques à l'activité de soins assurée, et déterminées par les fondateurs du réseau.

Ces dossiers doivent, bien entendu, respecter les règles et recommandations décrites ci-dessous, comme l'ensemble des dossiers informatisés contenant des données personnelles de santé.

4. Activités et Services médicaux hors champ de la médecine de soins

Nous visons notamment les services de contrôle médical de l'assurance maladie, de santé-sécurité au travail, d'assurances de personnes, de santé scolaire, de médecine d'expertise. Certes, les médecins de ces structures ont des statuts différents mais ils ont un point commun, celui d'intervenir, dans le cadre de leur mission, sur des situations individuelles. Le contenu du dossier doit être adapté aux missions et aux contraintes réglementaires auxquelles est astreint le médecin concerné. Il doit comporter l'ensemble des éléments qui contribuent à l'élaboration de sa décision.

4.1 Le médecin du travail et le médecin de prévention

- Au moment de l'embauche, le médecin du travail établit un dossier médical qu'il complètera lors des visites ultérieures[1]. Les règles relatives au secret vis-à-vis de l'employeur ou des personnels administratifs de la structure de médecine du travail s'appliquent (article R.4127.104 du Code de la santé publique).

- Ce dossier peut également être alimenté et consulté par les personnels infirmiers du travail, collaborateurs du médecin du travail, sous sa responsabilité et avec son accord, dans le respect du secret professionnel et dans la limite de ce qui est strictement nécessaire à l'exercice de leur mission.

- Le dossier peut également être consulté par :

  - le travailleur ou, en cas de décès du travailleur, par toute personne autorisée par la réglementation en vigueur (consultation des seuls éléments transmissibles),
  - le médecin inspecteur régional du travail et de la main d'œuvre (consultation de tous les éléments du dossier),
  - un autre médecin du travail afin d'assurer la continuité de la prise en charge, sauf refus du travailleur dûment informé au préalable (consultation de tout ou partie des informations selon les cas),
  - d'autres médecins désignés par le travailleur (consultation des seuls éléments transmissibles).

- Ce dossier est composé de diverses informations :

  - socio-administratives,
  - concernant l'emploi,
  - concernant la santé des travailleurs,
  - propositions et avis du médecin du travail.

Si le dossier médical est informatisé, il doit respecter les conditions de sécurité décrites ci-dessous comme pour l'ensemble des dossiers informatisés contenant des données personnelles de santé.

[1] Article D 4624-46 du Code du travail

4.2 Le médecin scolaire : médecin de dépistage et de prévention

- Le médecin scolaire est un professionnel de santé de l'Education nationale.
- Les observations du médecin scolaire sont inscrites sur le dossier médical scolaire ainsi que sur le carnet de santé, qui possèdent tous deux un caractère confidentiel. Les parents ou représentants légaux de l'élève peuvent avoir accès au dossier médical dans les conditions prévues à l'article L.1111-7, 5ème alinéa du code de la santé publique.
- Lorsque des problèmes de santé ont été repérés, les médecins de l'Education nationale travaillent en lien avec l'équipe éducative et les professionnels de santé afin que, pour chaque enfant, une prise en charge et un suivi adaptés soient réalisés.

Dès lors que le dossier médical scolaire est informatisé, il doit obligatoirement respecter des conditions de sécurité propres à en assurer la confidentialité.

4.3 Le médecin conseil de l'Assurance maladie

- Le praticien-conseil du service du contrôle médical, et les personnes placées sous son autorité, n'ont accès aux données de santé à caractère personnel que si elles sont strictement nécessaires à l'exercice de leur mission, dans le respect du secret médical[2].
- Est alors reconnu, au nom du principe du secret partagé dans le cadre d'une consultation médico-sociale, l'échange de renseignements entre le médecin traitant et le médecin-conseil, sauf opposition du patient[3].

L'échange de renseignements n'est autorisé qu'aux conditions suivantes :

- le patient doit avoir donné son accord,
- les renseignements doivent être communiqués, non au service de contrôle, mais à un médecin-conseil,
- le médecin traitant ne confie que les données indispensables au médecin-conseil pour que celui-ci puisse prendre sa décision,
- le médecin traitant reste juge de l'opportunité et de l'étendue des informations échangées.

En ce qui concerne le système d'information des organismes de protection sociale dans lesquels le médecin conseil exerce son activité, une distinction absolue doit être faite entre les données administratives ou de liquidation des prestations et les données du service médical. Les données du service médical sont des données personnelles de santé.
Les règles énoncées aux chapitres suivants s'appliquent.
Si le dossier médical est informatisé, il doit respecter les conditions de sécurité rappelées plus loin comme pour tous les dossiers médicaux.

[2] Article L 315-1 du Code de la sécurité sociale
[3] Articles R 4127-50 et R4127-104 du Code de la santé publique

B. La transmission, la conservation et l'archivage du dossier médical

1. La transmission

« Tout médecin doit, à la demande du patient ou avec son consentement, transmettre aux médecins qui participent à sa prise en charge ou à ceux qu'il entend consulter, les informations et documents utiles à la continuité des soins.
Il en va de même lorsque le patient porte son choix sur un autre médecin traitant. »
(Article 45 du Code de déontologie médicale)
Ce principe s'applique en établissements de santé comme en cabinet de ville.

En cas de cessation d'activité du médecin libéral :

Les patients doivent être avertis de la cessation d'activité de leur médecin, qu'elle soit causée par son départ en retraite, une indisponibilité, un changement d'orientation dans sa carrière professionnelle, ou provoquée par son décès.

Les dossiers médicaux seront alors :

- transmis par le médecin à son successeur, sous réserve du libre choix du patient,

- transmis aux médecins désignés par le patient, si le médecin n'a pas de successeur. Il restera cependant, à l'issue de ce processus qui peut durer quelques mois, et après un tri des dossiers les plus anciens, un reliquat de dossiers dont le médecin devra assurer l'archivage.

- Le médecin doit s'assurer que la continuité des soins est garantie en informant son conseil départemental du lieu où sont conservés les dossiers médicaux, ce qui permettra d'orienter les patients désireux d'y accéder.

- Lorsque l'interruption d'exercice est soudaine, le conseil départemental apportera son aide à la famille du médecin qui se trouve dans l'incapacité d'organiser lui-même la transmission des dossiers aux confrères désignés par les patients. Cependant, l'archivage du reliquat des dossiers relèvera de la responsabilité des ayants droit du médecin.

En cas de cessation d'activité du médecin de l'établissement de santé :

- Le médecin ne peut emporter les dossiers de ses patients, leur conservation incombant réglementairement à l'établissement. Cependant, il peut consulter ces dossiers après son départ, soit pour suivre un malade, dans un autre lieu ; soit dans le cadre d'une activité d'enseignement et de recherche.

2. La conservation des dossiers actifs

- Les dossiers médicaux établis par les médecins libéraux sont conservés sous leur responsabilité.

- Les dossiers médicaux tenus en établissement de santé sont conservés dans les services de l'hôpital, sous la responsabilité du médecin chef de service.

- L'un des premiers bénéfices de l'informatisation des dossiers réside dans l'encombrement réduit comparé au support papier. Les dossiers numérisés sont alors conservés soit sur le poste du médecin, en exercice libéral, soit sur un serveur commun, en cabinet de groupe, en réseau, ou en établissement ou dans les activités et les services médicaux hors champ de la médecine de soins, soit en solution d'hébergement conforme au décret hébergeur

Dans tous les cas, des dispositifs propres à garantir la confidentialité des informations que ces dossiers contiennent doivent être mis en œuvre.

3. L'archivage

- En l'absence de prescription juridique déterminant la **durée de conservation des archives des médecins libéraux**, il était d'usage de conseiller un archivage de trente ans, durée essentiellement alignée sur le délai de prescription en matière civile.

- L'article L 1142-28 du Code de la santé publique, issu de la loi du 4 mars 2002, a bien ramené le délai de prescription à dix ans mais ce délai court à compter de la consolidation du dommage et n'est applicable qu'aux actes et préjudices causés à compter du 5 mars 2002.

- La durée de conservation des archives hospitalières est fixée à vingt ans à compter de la date du dernier séjour – ou de la dernière consultation externe – du patient dans l'établissement, sous réserve du cas particulier des mineurs[4].

- Cette nouvelle disposition souligne que la durée de conservation n'est pas déterminée en fonction de la durée de prescription en matière de responsabilité médicale, mais justifiée par des considérations essentiellement médicales, la nécessité de conserver les preuves nécessaires à toute défense utile du médecin comme du patient et de garantir le droit d'accès des patients aux informations de santé les concernant.

- Le Conseil national de l'Ordre des médecins conseille aux médecins libéraux de s'aligner sur le délai minimal de 20 ans appliqué par les établissements de santé.

4. Article R.1112-7 du code de la santé publique

- L'archivage des dossiers « papier » tenus par les médecins libéraux peut être réalisé soit par le médecin lui-même, ce qui peut se révéler une source d'encombrement, soit par une société spécialisée engagée par contrat.
- Si le dossier est informatisé, un archivage sur disque optique numérique est à privilégier, bien qu'il souffre encore aujourd'hui d'une carence importante dans la durée. A ce propos, rien n'interdit au médecin libéral de déposer ses dossiers auprès d'un hébergeur agréé, comme cela est prévu pour les dossiers tenus par un établissement de santé.

- Les dossiers médicaux « papier » ou informatisés doivent être archivés dans des conditions permettant d'assurer leur confidentialité et leur pérennité.

- Les dossiers médicaux tenus en établissement de santé peuvent être soit conservés au sein des établissements eux-mêmes, soit déposés auprès d'un hébergeur agréé[5], ce qui implique alors qu'ils aient été informatisés.

L'archivage des documents numériques soulève une question relative à leur valeur probante : l'écrit sous forme électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et à préciser la date de création du document[6].

Le CNOM recommande en outre d'opter pour des systèmes de stockage horodatés, garants de l'intégrité du document numérique. Le CNOM demande aux agences de l'Etat d'établir avec les industriels du secteur informatique des règles opposables assurant la pérennité de lecture des formats et d'utilisation des supports afin de permettre l'exploitabilité des données dans le temps.

II. Les règles propres au dossier médical informatisé

A. La déclaration à la CNIL

Dispositions générales

- Le dossier médical informatisé constituant un traitement de données à caractère personnel susceptible de porter atteinte aux libertés et à la vie privée du patient, **il doit obligatoirement faire l'objet d'une déclaration auprès de la CNIL[7]** sous peine de sanctions.

Déclaration des traitements de données à caractère personnel mis en œuvre par les médecins libéraux

- Il incombe au médecin libéral de déclarer les traitements automatisés de données personnelles qu'il met en œuvre.

[5] Article R 1112-7 du Code de la santé publique
[6] Arrêt de la 2ème chambre civile de la Cour de cassation du 4 décembre 2008 n° pourvoi 07-17.622
[7] Article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- La CNIL a adopté une norme simplifiée (norme n°50), le 22 novembre 2005[8], qui offre une procédure de déclaration simplifiée des traitements automatisés de données personnelles : elle peut être directement réalisée en ligne via le site internet de la CNIL.

- Cette norme, précise que « les informations enregistrées ne peuvent être conservées dans l'application au-delà d'une durée de cinq ans à compter de la dernière intervention sur le dossier. A l'issue de cette période, elles sont archivées sur un support distinct et peuvent être conservées pendant quinze ans dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application. »

Le CNOM considère que cette durée est trop courte dans l'exercice pratique de la médecine et recommande à la CNIL d'en adapter l'application au monde de la santé. En toutes hypothèses, il reviendra aux éditeurs de logiciels médicaux, pour l'exercice en cabinets comme en établissements, d'intégrer la norme dans les fonctions automatiques des logiciels. Le CNOM prendra l'attache des organisations fédératives des éditeurs afin d'y pourvoir.

Déclaration des traitements de données à caractère personnel mis en œuvre par les établissements de santé

- Les déclarations sont adressées par l'établissement de santé à la CNIL, qui dispose alors d'un délai de deux mois pour délivrer le récépissé de déclaration constituant le feu vert pour la mise en œuvre d'un fichier ou d'un traitement automatisé de données personnelles.

Les établissements de santé sont encouragés, comme les collectivités locales et les entreprises, à désigner un CIL, Correspondant Informatique et Libertés. Le CNOM soutient cette recommandation. L'existence de cette fonction présente un double intérêt :
- bénéficier d'un allégement des obligations en matière de formalités préalables,
- disposer d'un expert capable de garantir la sécurité juridique et informatique. Vis-à-vis de l'extérieur, il témoigne de l'engagement de l'hôpital en faveur du respect de la vie privée et des droits des personnes et représente un gage de confiance.

B. Les obligations incombant au responsable d'un traitement automatisé de données

L'obligation d'information[9]

- Avant de mettre en œuvre un fichier ou un traitement automatisé de données personnelles, **le médecin ou l'établissement doit en informer le patient** (affichette dans la salle d'attente, document d'entrée en établissement …). Le CNOM en publiera un modèle type.

[8] Délibération de la CNIL n° 2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet
[9] Article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

L'obligation de sécurité et de confidentialité[10]

- « Le responsable est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Le CNOM rappelle que les personnels administratifs des établissements ou des organismes de protection sociale ne sont pas des tiers autorisés à accéder aux données médicales.

- Les précautions prises par les professionnels de santé dans le cas des dossiers « papier » sont jugées insuffisantes par la CNIL en ce qui concerne une informatisation généralisée des dossiers médicaux.

La CNIL recommande, comme le CNOM, de mettre en place un dispositif de sécurité adéquat et d'observer des habitudes de prudence (en matière de gestion des mots de passe par exemple, ou de sauvegardes).

C. Le droit d'opposition[11] et de rectification[12]

« Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que les données à caractère personnel la concernant fassent l'objet d'un traitement ».
(Article 38 de la loi relative à l'informatique, aux fichiers et aux libertés)

« Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. »
(Article 40 de la loi relative à l'informatique, aux fichiers et aux libertés)

- La CNIL considère que la demande d'un patient qui concernerait l'effacement de données qui ne seraient ni inexactes, ni incomplètes, ni équivoques ou périmées, ne peut être satisfaite, sauf si le patient invoque des motifs légitimes.

Le CNOM recommande que l'échange entre le médecin et le patient soit le moyen le plus raisonnable d'apprécier le caractère périmé d'une information. En toute hypothèse, le médecin doit agir en conscience, le patient restant libre de saisir le juge en cas de désaccord.

[10] Article 34 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[11] Article 38 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[12] Article 40 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Dans le cas où l'effacement d'une donnée est décidé de façon conjointe par le patient et le professionnel de santé, aucune technique particulière n'est exigée par la CNIL. Le CNOM s'associe à la recommandation de la CNIL qui stipule que la mention de cette suppression soit conservée dans le fichier

Le CNOM recommande que la suppression fasse l'objet d'une demande formalisée par écrit de la part du patient et que le médecin en conserve l'original.

D. L'hébergement des dossiers actifs

- Les professionnels de santé ou les établissements de santé peuvent déposer des données de santé à caractère personnel auprès d'un hébergeur agréé.
- Cet hébergement ne peut avoir lieu qu'avec le consentement exprès de la personne concernée.
- La prestation d'hébergement doit faire l'objet d'un contrat entre le professionnel de santé, ou l'établissement de santé, et la société d'hébergement.
- S'agissant de l'accès à ces données par le professionnel de santé, ou l'établissement de santé, qui les a déposées, le consentement de la personne concernée n'est pas requis[13].
- Les hébergeurs doivent mettre en place une série de conditions propres à assurer la pérennité, la confidentialité et la sécurité des données de santé à caractère personnel[14].
- Ils sont tenus de les mettre à la disposition des personnes autorisées, selon des modalités définies par contrat, et de les restituer en fin de contrat.
- L'agrément d'une société d'hébergement est délivré par le ministre chargé de la Santé, après avis motivé d'un comité d'agrément et de la CNIL, pour une durée de trois ans.

III. Les règles relatives au dossier médical informatisé et partagé

Si l'informatisation du dossier médical a, historiquement, répondu à des besoins administratifs et de gestion, ce n'est plus, actuellement, la seule motivation.
La numérisation des données prend en effet une nouvelle dimension, dans l'intérêt même du patient, avec des objectifs de partage, qui se trouve ainsi facilité et accéléré, au bénéfice de la coordination des soins. Toutefois, ce partage doit faire l'objet du recueil du consentement exprès préalable du patient, hormis le cas d'urgence ou d'impossibilité.

Si l'on doit concevoir des « passerelles » entre les deux, le dossier médical informatisé partagé, à vocation professionnelle, est distinct du dossier médical personnel (DMP), propriété de l'assuré, annoncé par la loi d'août 2004.

[13] Article L 1111-8 alinéas 1, 2 et 5 du Code de la santé publique
[14] Article R 1111-9 du Code de la santé publique

A. Le partage en cabinet médical et en organisations pluri-professionnelles

- Au sein d'une structure mono disciplinaire, les dossiers médicaux informatisés des patients sont le plus souvent stockés sur un serveur commun. Ils peuvent faire, de fait, l'objet d'un partage entre les différents médecins. En l'absence de l'un d'eux par exemple, il est alors plus facile d'assurer la continuité des soins au patient.

Le CNOM recommande que le patient soit informé de ce partage afin d'exercer son droit de choisir librement son médecin, ainsi que son droit d'opposition, le cas échéant.

- Dans une structure pluridisciplinaire, chaque médecin ayant sa propre patientèle, les dossiers médicaux des patients ne peuvent pas être partagés entre les professionnels de santé.

Si les dossiers informatisés sont stockés sur la même base, le CNOM recommande une gestion par habilitation avec la conservation des traces historiées des accès.

Toutefois, si plusieurs médecins interviennent dans la prise en charge d'un patient, son dossier médical sera partagé, sauf s'il s'y oppose.

- Le cas d'une structure pluri professionnelle, regroupant à la fois des professionnels médicaux et des professionnels de santé, est sans doute appelé à se développer sur les territoires de santé, soit sous la forme d'une maison de santé soit sous la forme d'un pôle regroupant des cabinets distincts mis en réseau par informatique. Le CNOM recommande que chaque profession dispose volet qui lui soit propre dans un logiciel commun à la structure et que, en toutes hypothèses, les différents volets ne puissent faire l'objet d'un partage que sous réserve de l'information préalable du patient, de son consentement et de son droit d'opposition. Ce point fera l'objet d'une communication spécifique une concertation étant en cours avec les autres ordres des professions de santé.

Partage des dossiers: recommandations du CNOM

Si le partage du dossier médical devient nécessaire afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible, son informatisation facilite son accès par les professionnels de santé concernés par cette coordination.

- Le dossier médical peut alors être stocké sur un serveur commun à la structure et les professionnels de santé y accèdent par le biais d'un moyen assurant leur identification certaine.

- Cependant, dans le cas du décès de l'un des professionnels par exemple, se pose une difficulté d'accès à ses dossiers par ses confrères, son identifiant et son mot de passe n'étant pas connus des autres associés. Il est donc recommandé que chaque médecin confie son identifiant et son mot de passe, sous pli fermé, au Conseil départemental au tableau duquel il est inscrit, afin que l'accès aux dossiers d'un médecin décédé puisse avoir lieu sans difficulté.

- La mise en commun des dossiers sur un serveur unique peut soulever une difficulté en cas d'arrêt de l'activité de l'un des médecins au sein de la structure : de quelle façon le professionnel cessant son activité pourra-t-il récupérer les dossiers qu'il a établis ? Dans les associations de praticiens et dans les sociétés civiles de moyens, la règle de l'exercice personnel de chacun veut que les fichiers soient nominativement affectés. Ainsi, chaque professionnel cessant son activité peut récupérer ses dossiers. Dans les sociétés civiles professionnelles ou dans les sociétés d'exercice libéral, les dossiers appartiennent à la société qui doit assurer leur conservation. Elles ne peuvent donc s'en dessaisir, mais l'ancien associé peut obtenir la copie des dossiers qu'il avait constitués.

B. Le dossier unique en établissement de santé

- La réglementation établit que le dossier médical tenu en établissement de santé est un dossier commun à l'ensemble des professionnels de l'établissement qui participent à la prise en charge d'un patient. Il regroupe et formalise sur un même support l'ensemble des éléments se rapportant au patient. Chaque professionnel est astreint au secret attaché aux informations dont il a eu ou pu prendre connaissance.

- Chaque professionnel intervenant dans la prise en charge du patient complètera ainsi le dossier.

Le CNOM recommande que les dispositifs informatiques soient tels qu'ils puissent permettre, dans l'intérêt des patients comme des professionnels eux-mêmes, l'identification certaine des accès en lecture comme en écriture.

- Dès lors qu'une personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe[15].

- Le dossier « papier » peut parfois faire l'objet d'un accès trop aisé (chariot dans le couloir de l'établissement, bureau ne fermant pas à clé…) entraînant un manque de confidentialité des informations qui le composent. L'informatisation du dossier médical doit permettre d'offrir une plus grande confidentialité et la possibilité de gérer les droits d'accès permettant d'en limiter l'utilisation aux seuls professionnels habilités.

Le CNOM recommande que l'accès au dossier informatisé et la confidentialité des données qu'il renferme soient verrouillés par l'emploi d'un moyen assurant l'identification de l'accédant, que le dossier soit stocké sur le poste du professionnel de santé ou sur un serveur commun à l'établissement. Le CNOM recommande une traçabilité des accès et la conservation indéfinie du journal des traces.

La CNIL préconise l'adoption de mesures de sécurité physique et logique adaptées à l'utilisation qui est faite de l'ordinateur, sa configuration, sa connexion ou non à l'Internet. **Elle conseille de chiffrer les données figurant sur le disque dur et sur les supports de sauvegarde**. Selon le CNOM, la sécurité relève d'un ensemble de mesures associées entre elles, dont le chiffrement qui reste un élément majeur.

C. Le DMP

Le Dossier Médical Personnel est prévu pour constituer un ensemble de services permettant au patient, qui l'aura librement accepté, et aux professionnels de santé qu'il a autorisés, de partager sous forme électronique des informations de santé en vue d'améliorer la prévention, la continuité, la coordination et la qualité des soins. **Le DMP ne va pas se substituer au dossier « métier » du professionnel de santé, ni aux dossiers d'établissements, mais s'articuler étroitement avec eux.**

Sous le couvert du consentement du patient, il sera alimenté par tout document que le professionnel de santé juge utile à la coordination des soins.
Il est prévu une articulation fonctionnelle avec le Dossier pharmaceutique et l'historique des remboursements.

Il pourra être fermé à la demande d'un patient, et sera alors archivé sur une période de 10 ans.

Il fera l'objet d'un hébergement national assuré par un consortium industriel sous la tutelle de l'ASIP Santé.

Les décrets relatifs au DMP sont en cours d'élaboration. Le CNOM participera attentivement à la concertation dans leur écriture.

[15] Article L 1110-4 alinéa 3

L'accès au dossier médical

I. Les règles communes au dossier médical « papier » et au dossier médical informatisé

A. Le secret entourant le dossier médical

- Le secret, et de manière plus spécifique le secret médical, est régi par deux dispositions principales :

  - ☛ Article 4 du Code de déontologie médicale, (R.4127-4 du CSP)
  - ☛ Article L 1110-4 du Code de la santé publique.

- Le secret médical couvre toutes les données à caractère personnel concernant le malade, de son identité aux différents documents médicaux.

- Sont tenus au secret professionnel :

  - ☛ les professionnels de santé,
  - ☛ les professionnels intervenant dans le système de santé,
  - ☛ les personnes qui assistent le médecin (secrétaire médicale par exemple).

- La violation du secret médical est punie d'un an d'emprisonnement et de 15 000 euros d'amende[16].

- Le secret partagé est prévu par l'article L 1110-4 alinéa 3 du Code de la santé publique qui précise que : « Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible … ».

  Le consentement du patient est donc nécessaire en préalable à cet échange d'informations.

  Le secret partagé s'applique également entre les médecins des secteurs de soins et les médecins-conseils de l'Assurance-maladie, dans le cadre de l'instruction et la gestion des éléments nécessaires à l'obtention des avantages sociaux ou prestations auxquels le patient a droit. Le CNOM rappelle que les médecins-conseils sont astreints au secret médical vis-à-vis des services administratifs et financiers de l'Assurance-maladie auxquels ils ne doivent communiquer que les conclusions de l'instruction médicale des dossiers. Les dispositifs informatiques internes doivent donc permettre la préservation de cette exigence déontologique.

Le respect du secret entourant le dossier médical peut être pleinement assuré quand il est informatisé.

[16] Article 226-13 du Code pénal

B. L'accès du patient au dossier médical

Peuvent demander l'accès au dossier médical :

- la personne concernée par les données,

- ou ses ayants droit, en cas de décès, afin de leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès,

- ou la personne ayant l'autorité parentale si le patient est mineur,

- ou le tuteur si le patient est un majeur protégé,

- ou, le cas échéant, le médecin qu'une de ces personnes a désigné comme intermédiaire[17].

De même que pour le dossier « papier » dont il est délivré copie, le dossier informatisé fera l'objet d'une édition papier, ou sur un support informatique mobile assurant l'inaltérabilité des données inscrites, qui sera remise aux demandeurs qualifiés.

C. La saisie des dossiers médicaux

- Les perquisitions et saisies dans les cabinets médicaux sont soumises à des règles strictes, en raison du secret qui s'attache aux informations détenues par les professionnels de santé.

Si la **perquisition** est toujours réalisée par le magistrat qui la décide (article 56-3 du code de procédure pénale) il est admis que la saisie d'un dossier médical, parfaitement identifié, puisse être effectuée par un officier de police judiciaire agissant sous le contrôle du procureur de la République ou sur commission rogatoire du juge d'instruction.

La **saisie** sera opérée en présence du médecin requis, le cas échéant du directeur de l'établissement public et du représentant de l'Ordre des médecins qui s'assurera que n'est saisi que le dossier concerné.
Le dossier est inventorié et placé sous scellés fermés.

- Saisie d'un document informatisé

« Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice, soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition. » (article 97, 3ème alinéa du code de procédure pénale)

La copie sur papier, CD rom ou clé USB, d'un dossier médical parfaitement identifié et sous réserve que le médecin responsable le sélectionne, est effectuée dans des conditions comparables à celle d'un dossier papier.

[17] Article R 1111-1 du Code de la santé publique

- Demande de documents et listes

Depuis les lois Perben de 2003 et 2004, le procureur de la République ou l'OPJ, sur l'autorisation de celui-ci (enquête préliminaire – article 77-1-1 du code de procédure pénale) ou sous son contrôle (enquête de flagrance – article 60-1 du même code) « *peut requérir de toute personne, de tout établissement ou organisme privé ou public, de toute administration qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposé, sans motif légitime, l'obligation au secret professionnel*. »

Lorsque la réquisition est adressée à une des trois catégories professionnelles : avocat, journaliste, **médecin** (visées respectivement aux articles 56-1 à **56-3** du code de procédure pénale), les articles 77-1-1 et 60-1 ajoutent que la remise des documents ne peut intervenir qu'avec l'accord du professionnel concerné.

Ces articles font donc dépendre la remise d'un dossier couvert par le secret médical de l'accord du médecin, ce qui paraît incompatible avec la conception traditionnelle du secret professionnel général et absolu en matière médicale.

Les dispositions des articles 77-1-1 et 60-1 sont de plus en plus souvent invoquées –parfois de manière incomplète – par les OPJ pour obtenir –sans saisie- les documents qu'ils détiennent.

Il faut conseiller aux médecins requis dans cette situation de refuser leur accord. **Ce refus ne peut être sanctionné.** La procédure de saisie sera alors mise en œuvre dans les conditions habituelles (présence d'un conseiller ordinal, mise sous scellés fermés du dossier saisi) éventuellement opérée par le magistrat lui-même.

Le CNOM rappelle que :

- la réquisition n'a pas pour effet de délier un médecin du secret professionnel,
- un médecin ne peut, de son propre chef, se délier du secret professionnel auquel il est tenu et donner son accord à la remise de documents concernant les patients à un officier de police judiciaire,
- lorsqu'il est requis de remettre des documents ou de communiquer des informations concernant la santé d'une personne, le médecin doit opposer un refus et demander l'application de la procédure de saisie,
- les dossiers médicaux seront alors saisis en présence d'un magistrat, ou de l'officier de police judiciaire délégué à cette fin, du médecin responsable et d'un représentant de l'Ordre des médecins. Ils seront placés sous scellés.
- dans le cas d'un dossier médical informatisé, la saisie d'une partie du fichier, voire du disque dur, doit être assimilée à une perquisition et doit être faite par un magistrat en présence de la personne responsable de l'Ordre des médecins.

II. Les règles propres au dossier médical informatisé et partagé

Le développement des prises en charge multi disciplinaires et les progrès des technologies de l'information ont conduit à transformer les modes de gestion des données de santé.

A l'heure actuelle, un médecin est fréquemment amené à utiliser, outre sa propre application locale de gestion des dossiers médicaux, un grand nombre d'applications extérieures renfermant des données de santé : dossiers de réseaux, de plates-formes régionales, dossier communicant de cancérologie, historique de remboursements, dossiers de pôles de santé…

Le CNOM recommande, face à cette multiplicité d'interventions professionnelles d'exiger l'observation de règles précises et unifiées relatives au consentement du patient et celles qui concernent les droits d'accès et la traçabilité de ces accès.

Un professionnel de santé ne peut accéder au dossier médical informatisé partageable d'un patient que si celui-ci ne s'y est pas opposé[18], et en fonction des habilitations qui lui ont été accordées. L'accès peut être réalisé par l'utilisation de la carte de professionnel de santé, ou un dispositif équivalent.

La protection des données de santé passe également par la vérification du contrat d'assistance et de maintenance qui lie le cabinet médical à son éditeur de logiciel, et de façon générale à tout fournisseur de services informatiques. Il doit comporter une clause de confidentialité rappelant leurs obligations à ces sociétés, comme le préconise la CNIL.

A. La gestion des droits d'accès des professionnels de santé

- En fonction de leur profession, de leur rôle et de leurs missions dans l'équipe de soins, les professionnels de santé se voient accorder, **sous le régime du consentement du patient**, un accès en mode « lecture/consultation » et/ou en mode « écriture/alimentation ».
- Seuls les professionnels de santé bénéficiant d'un droit d'accès en mode « écriture/alimentation » pourront déposer, sous leur responsabilité, des données de santé à caractère personnel dans le dossier informatisé partagé d'un patient. Il s'agit donc de mettre en place un système d'habilitation propre à n'autoriser le mode « écriture/alimentation » qu'à certains professionnels identifiés.
- S'agissant du mode « écriture/alimentation » :

  - ☛ le consentement du patient à chaque alimentation est exclu,
  - ☛ pour autant, le patient doit pouvoir exercer son droit d'opposition au dépôt de toute donnée,
  - ☛ tout professionnel de santé autorisé à accéder au dossier peut l'alimenter en données pertinentes pour la coordination des soins.

[18] Article L 1110-4 alinéa 3 du Code de la santé publique

- Concernant le mode « lecture/consultation » :

  - ☛ l'organisation des habilitations et des données accessibles en fonction de leur degré de confidentialité doit être optimisée pour rendre les règles d'accès compréhensibles de tous,
  - ☛ l'accès en « lecture/consultation » d'un professionnel de santé est conditionné par l'autorisation qui lui est donnée.

B. La traçabilité des accès

- La traçabilité des connexions par proxy, caches ou pare-feu, correspond à une procédure de journalisation.

- La journalisation des connexions consiste à identifier et enregistrer toutes les connexions ou tentatives de connexions à un serveur de bases de données afin que soient assurées la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés, ni utilisées à des fins étrangères à celles qui justifient leur traitement.

- Lorsque les fichiers de journalisation permettent de collecter des informations individuelles poste par poste afin de contrôler l'activité des utilisateurs, ils doivent être déclarés à la CNIL.

- Les professionnels de santé doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardées.

C. La communication du dossier médical

- La communication du dossier médical est soumise aux mêmes règles de procédure, qu'il s'agisse d'un dossier « papier » ou d'un dossier informatisé.

- Avant toute communication du dossier médical, le médecin doit s'assurer de l'identité du demandeur[19].

- Le demandeur obtient du professionnel de santé, ou de l'établissement de santé, communication des informations

  - ☛ soit par consultation sur place, avec, le cas échéant, remise de copies de documents,
  - ☛ soit par l'envoi de copies des documents. Les frais de délivrance de ces copies sont laissés à la charge du demandeur.

[19] Article R 1111-1 alinéa 3 du Code de la santé publique

- Dans le cas où les informations requises sont détenues par un établissement de santé, et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter par voie électronique tout ou partie des informations en cause[20].

  Cette disposition pourrait également s'appliquer dans le cas d'un cabinet libéral.

  Si les informations sont hébergées, leur communication sera obligatoirement réalisée par le professionnel de santé ou l'établissement de santé dépositaires de ces données.

D. L'accès au DMP

- L'accès du patient à son DMP se fera progressivement, dans le cadre du processus de relance annoncé en 2009 par le ministère de la Santé et confié à l'ASIP Santé.

- Le CNOM rappelle que l'ouverture d'un DMP ne porte aucun caractère obligatoire, le ministère ayant suivi en cela l'avis qu'il avait sollicité du Comité national consultatif d'éthique. **Le DMP est un dossier personnel propre au patient. Il ne se confond pas avec les dossiers professionnels**. Selon le CNOM, il ne devrait comporter que des données pertinentes et structurées nécessaires à la coordination des parcours de soins et aux coopérations des professionnels plus que le suivi analytique des épisodes de soins.

- Le patient lui-même pourra consulter son DMP via une interface web, en utilisant une authentification forte (identifiant + mot de passe à usage unique). Il pourra consulter tous les documents – et toutes les traces d'accès à ces documents - sauf dans le cas des documents sensibles (avant consultation d'annonce notamment).

- Il pourra masquer des documents. Selon le CNOM, ce masquage informatique est l'équivalent du silence lors de l'interrogatoire qui compose l'examen clinique. Il renforce la responsabilité personnelle du patient en ce sens que le masquage informatique « tracé » apporte la preuve que le patient a tu un évènement et que, par conséquent, il ne pourrait être reproché au médecin ne pas l'avoir su lors de sa prise de décision.

- Le patient pourra également utiliser le DMP pour :

  - ☛ alimenter son espace d'expression personnelle (souhaits en matière de dispositions de fin de vie, par exemple)
  - ☛ correspondre de façon sécurisée avec un professionnel de santé, dès lors que ce dernier a donné son accord.
  - ☛ gérer les droits d'accès à son DMP
  - ☛ demander la restitution ou la fermeture de son DMP.

[20] Article R 1111-2 alinéa 2 du Code de la santé publique

En dehors des accès prévus par la loi, et des habilitations données par le patient, toute tentative d'accès au DMP sera interdite et sanctionnée pénalement.

L'accès des professionnels de santé au DMP se fera via le logiciel du professionnel ou via une interface web, uniquement après authentification.

L'authentification sera réalisée :

- soit directement, avec une carte de professionnel de santé (ou un dispositif équivalent) ; elle permettra alors l'alimentation et la consultation du DMP,

- soit indirectement, avec un certificat d'établissement ; elle permettra uniquement l'alimentation du DMP. Une procédure de « bris de glace » sera toutefois prévue pour les accès en urgence.

Les habilitations de consultation accordées aux différentes catégories de professionnels de santé seront établies par une matrice d'habilitation.

Les échanges par voie électronique

I. La confidentialité dans les échanges électroniques de documents

Fondements du secret de la correspondance :

- *« Le médecin doit veiller à ce qu'aucune atteinte ne soit portée par son entourage au secret qui s'attache à sa correspondance professionnelle. » (*Article R 4127-72 du Code de la santé publique, Article 72 du Code de déontologie médicale)
- Droit au respect de la correspondance. Article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.
- La violation de la correspondance est punie d'un an d'emprisonnement et de 45 000 euros d'amende (Article 226-15 du Code pénal).
- Les échanges par voie de télécommunication sont couverts par le secret de la correspondance et leur interception, détournement, divulgation sont sanctionnés des peines prévues à l'article 226-15 du code pénal.
- Les correspondances entre médecins pouvant comporter des données médicales soumises au secret professionnel, « le médecin doit protéger contre toute indiscrétion les documents médicaux, concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents »[21].
- Ces correspondances constituent des pièces du dossier médical et sont régies par les règles du secret médical partagé[22].

[21] Article R 4127-73 du Code de la santé publique (Article 73 du Code de déontologie médicale)
[22] Article L 1110-4 alinéa 3 du Code de la santé publique

Echanges électroniques de documents

- La confidentialité des informations médicales transmises par voie électronique est encadrée par l'article L1110-4 du code de la santé publique et le décret du 15 mai 2007 toujours en vigueur, relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. Une révision de la rédaction du décret a été annoncée.

- Le CNOM recommande que les nouvelles dispositions règlementaires soient adaptées aux usages professionnels mais qu'elles garantissent également fortement aux patients et aux professionnels les sécurités déontologiques attachées à de la protection des données personnelles de santé appelées à circuler.

- Le CNOM considère que le développement de l'utilisation de messageries professionnelles sécurisées constitue un pré requis à l'objectif d'échange et de partage des informations nécessaires à la qualité des soins.

- Ces messageries sécurisées, **dédiées aux usages professionnels**, faciliteront notamment les échanges ville - hôpital, condition nécessaire à une meilleure coordination des soins. Cela suppose une interopérabilité indispensable entre toutes les applications de messageries sécurisées.

Le CNOM rappelle que l'usage de messageries n'affecte pas le droit des patients à l'information qui leur est due par l'émetteur du courrier sur son intention de communiquer des éléments du dossier à un autre professionnel[23].

- Les messageries sécurisées garantissent :

  - ☛ l'identité, la qualité professionnelle et la validité de l'adresse électronique de leurs correspondants (identification),
  - ☛ l'intégrité du contenu du message jusqu'à sa réception et de son imputabilité (signature électronique),
  - ☛ la confidentialité des messages (chiffrement).
  - ☛ la non répudiation

- Tous les médecins appelés à échanger ou à partager des données de santé dans le parcours de soins d'un patient par l'utilisation des technologies de l'information et de la communication doivent être personnellement identifiés et authentifiés de façon certaine dans l'espace informatique et les documents circulant doivent être chiffrés.

[23] Article L 1110-4 alinéa 3 du Code de la santé publique

- Ces fonctions d'identification, d'authentification et de chiffrement peuvent s'appuyer sur le système de la carte de professionnel de santé ou un dispositif équivalent.

- Un dispositif conforme à ces exigences a été mis à l'étude par le CNOM en liaison avec les autres Ordres des professions de santé. Il prévoit le déploiement d'une carte professionnelle qui serait une évolution de l'actuelle carte ordinale, avec des fonctionnalités assurées par les certificats électroniques reconnus dans la sphère de la santé afin de permettre l'accès à diverses applications.

- **Pour s'inscrire dans un Espace de Confiance numérique - où le CNOM doit être une partie légitimement prenante en application de ses missions générales - les messageries sécurisées doivent être déployées en étant adossées à deux autres services :**

  - ☛ **un annuaire des adresses électroniques certifiées des médecins inscrits au tableau,**
  - ☛ **une traçabilité des flux de messagerie, comprenant un dispositif de notarisation, apportant à l'émetteur et au récepteur du courriel la preuve de l'échange.**

II. Les outils de la sécurité informatique

Pour le CNOM, **les sécurités des systèmes d'information en santé sont des exigences déontologiques**. La description analytique que nous faisons ci-dessous des outils de la sécurité informatique ne doit pas faire craindre au lecteur d'avoir à faire à un système complexe et chronophage. En effet, ces outils doivent être intégrés aux logiciels utilisés et s'exécuter de façon automatique par le système dans lequel le professionnel se sera identifié et authentifié par l'emploi de certificats électroniques.
Pour ce qui concerne la pratique en établissements, il peut être envisagé – à titre transitoire - un certificat serveur d'établissement, sous réserve que les praticiens qui y exercent soient bien inscrits aux Tableaux des ordres professionnels et détiennent un numéro d'identification dans le RPPS. Dans cette situation de certificats serveurs d'établissement, la responsabilité du chef d'établissement se trouvera directement engagée.
Le cas des internes est en cours de résolution, par le pré enregistrement aux tableaux mais, au demeurant, ils ne peuvent agir et intervenir que sous la responsabilité du médecin dont ils dépendent.
Le CNOM est également conscient que l'expression « les sécurités informatiques » comporte aussi les protections des systèmes contre les attaques de cybercriminalité, la non altération des données, la robustesse et la disponibilité des systèmes. En effet, la qualité de soins en dépend largement dès lors que, dans le suivi du patient, les informations et les documents sont totalement dématérialisés. Cet aspect fera l'objet d'un complément ultérieur au présent rapport.

A. L'identification

- L'identification correspond à la présentation de l'identité proclamée destinée à être vérifiée.

Dans le cadre de l'informatisation de la santé, l'identifiant est un outil permettant au professionnel de santé d'être reconnu par un serveur ou par une application lui donnant accès à des données numérisées.

- L'identification d'un utilisateur auprès de sites ou de serveurs accédés via internet peut laisser des traces appelés cookies. Il s'agit de petits fichiers texte déposés sur le disque dur par le serveur du site. Ils facilitent la navigation en enregistrant les préférences de l'utilisateur. Ils sont le plus souvent utiles et non dangereux. Il est cependant conseillé de les employer avec prudence d'autant que les navigateurs permettent de les désactiver facilement.

B. L'authentification

- L'authentification correspond à la vérification que l'identité réelle est bien celle qui est présentée.

- Le médecin s'authentifie par l'utilisation de la carte porteuse de certificats électroniques, ou d'un dispositif équivalent, et d'un code pin. Dans une application interne, ce dispositif doit aussi comporter un mode dégradé afin d'assurer un secours pour la permanence du service en cas de perte ou d'inusitabilité de la carte. Ce mode dégradé de secours comporte la saisie d'un identifiant et d'un mot de passe qui doit être sous le contrôle personnel de l'utilisateur et suffisamment complexe pour ne pas être deviné. Ce mot de passe doit, en outre, être régulièrement modifié par le médecin lui-même. Cette règle devrait s'appliquer dans la politique générale de sécurité des systèmes d'information, après analyse des risques à couvrir. La traçabilité des transactions en mode « bris de glace » doit naturellement être assurée.

- La carte de professionnel de santé, ou un dispositif équivalent, embarque un certificat d'authentification et un code PIN.

Une fois l'authentification du professionnel assurée, il accède aux données médicales informatisées et peut les transmettre par le moyen d'une messagerie sécurisée.

Après identification et authentification, l'association de l'identité de la personne avec ses habilitations est réalisée afin de déterminer si elle est autorisée ou non à accéder aux données. Pour le CNOM, l'authentification dure tant que dure le contact de la carte électronique dans le lecteur ouvrant l'application. Si le CNOM reconnait que la mobilité des médecins dans les établissements justifie soit l'usage d'une carte sans contact, soit une identification-authentification forte à l'inscription dans le système d'information et la génération d'un jeton d'une durée de vie paramétrable sur un dispositif mobile, il souligne que la pratique ambulatoire comporte également une forte mobilité, notamment mais non exclusivement, pour les médecins urgentistes.

- A l'avenir, les dispositifs biométriques devraient se développer à des fins de contrôle de l'identification et de l'authentification des professionnels, comme des patients. Ils sont soumis à l'autorisation de la CNIL.

C. Le chiffrement

- Il s'agit d'un procédé rendant un document illisible pour quiconque ne possède pas la clé de déchiffrement. Il préserve la confidentialité des données et permet de garantir le secret médical.
- Dans le monde de la santé, le chiffrement est exigé par le décret du 15 mai 2007, toujours en vigueur, relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. Or, les conditions d'application de ce décret devaient être définies par des arrêtés qui n'ont jamais été publiés. En outre, le mode technique du chiffrement n'est pas établi par les textes et ce sujet relève des compétences de l'ASIP Santé. Enfin, la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (HPST) a récemment introduit la notion de « dispositifs équivalents » à la carte de professionnel de santé qui n'a pas encore suffisamment pénétré dans les établissements.

Le CNOM recommande qu'au regard des garanties de préservation des données personnelles de santé d'une part, de facilitation des échanges ville – hôpital d'autre part, les dispositions relatives au chiffrement soient publiées pour pouvoir être rapidement mises en œuvre. Il n'entre pas dans les compétences ordinales de se prononcer sur la nature technique des référentiels, mais le CNOM souligne l'importance des situations concrètes d'usage et contribuera à la recherche de convergences pour garantir l'interopérabilité.

- L'exigence légale de chiffrement s'applique à la transmission par voie électronique entre professionnels de santé.
- Au regard de la déontologie médicale le chiffrement est un élément essentiel dans les échanges de courriels contenant des données personnelles de santé et le CNOM exclue l'envoi de messages non chiffrés. La sécurité comporte également l'identification-authentification de l'expéditeur et du receveur, par un tiers de confiance.

D. Le tiers de confiance ou prestataire de services de certification électronique

- Le prestataire de services de certification électronique correspond à « toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique [24] ».
- Les certificats électroniques remplissent la fonction de carte d'identité numérique. Il s'agit de fichiers électroniques structurés et normalisés renfermant la clé publique de leur titulaire et les informations associées. Ces informations sont rendues infalsifiables par le chiffrement avec la clé secrète de l'autorité de certification.

[24] Article 1 du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique

- Le prestataire de services de certification électronique remplit les missions suivantes :

  - ☛ enregistrer les demandes de certificats électroniques, vérifier l'identité des porteurs de ces certificats (autorité d'enregistrement),
  - ☛ générer le certificat, assurer la publicité des clés publiques au moyen de registres spécifiques (autorité de certification).

Dans le cadre du Répertoire Partagé des Professionnels de Santé (RPPS) et de l'infrastructure de gestion des clés, les Ordres sont reconnus comme autorités d'enregistrement pour les populations professionnelles qui les concernent et l'ASIP Santé comme autorité de certification.

- L'ASIP Santé assure la responsabilité de prestataire des services de certification électronique pour le secteur de la santé. Elle délivre les cartes de professionnel de santé dans lesquelles sont intégrés les certificats nécessaires à :

  - ☛ la non répudiation et l'intégrité des données, avec la signature électronique,
  - ☛ la confidentialité des données, par leur chiffrement,
  - ☛ l'authentification d'un professionnel de santé.

Elle agrée les dispositifs équivalents à la carte CPS, qu'il s'agisse des certificats embarqués sur d'autres supports, ou, selon l'expression des Ordres, les cartes ordinales porteuses de certificats électroniques.

E. L'horodatage

- L'horodatage est un processus permettant de lier une date et une heure précise, via une horloge de référence, à un évènement, une information ou une donnée informatique. L'horodatage implique un tiers de confiance.

- L'horodatage permet la mise en œuvre des quatre garanties suivantes :

- l'intégrité : la délivrance d'un jeton d'horodatage permet de sceller des données électroniques puisque toute modification des données horodatées romprait la correspondance avec le jeton d'horodatage,

- l'antériorité : la datation des données électroniques permet de démontrer qu'elles existaient à partir de la date et heure certifiées,

- l'exactitude : la date et l'heure sont établies à partir de sources de temps fiables corrélées entre elles par des mécanismes indépendants, éliminant ainsi toute possibilité de dérive temporelle

- l'opposabilité : la date et l'heure associées aux données sont validées par la signature d'un tiers de confiance, l'autorité d'horodatage, dont l'indépendance protège de toute contestation liée au temps.

- Le médecin doit horodater ses feuilles de soins électroniques, mais il pourrait également utiliser l'horodatage pour établir ses ordonnances ou tout autre document dont il considère que l'intégrité doit être respectée.

F. La signature électronique

- La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie[25].

- Le procédé de signature électronique est présumé fiable, jusqu'à preuve du contraire, lorsqu'il met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié[26].

- La signature électronique sécurisée est basée sur la cryptologie asymétrique : deux clés distinctes sont utilisées, l'une pour chiffrer le message, la clé publique, et l'autre pour le déchiffrer, la clé privée. Ainsi, chaque utilisateur dispose des deux clés, l'une publique, qu'il distribue et l'autre privée, qu'il conserve.

- La signature électronique, produite par la carte de professionnel de santé ou un dispositif équivalent, est reconnue par les administrations de l'Etat et les organismes de Sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé[27].

- La signature électronique, qui tend à se généraliser dans d'autres domaines, juridiques notamment, pourrait être utilisée dans le cadre des certificats médicaux, ordonnances, attestations, ou tous documents délivrés par le médecin, afin de limiter les risques de falsification. Le CNOM vient de mettre en chantier un travail de concertation sur le développement de la prescription électronique, permettant la dématérialisation sécurisée de la chaine « prescription médicale >délivrance pharmaceutique>remboursement par les caisses d'assurance maladie ».

- Elle est également nécessaire pour sécuriser la transmission d'informations médicales par messagerie sécurisée.

[25] Article 1316-4 du Code civil
[26] Article 2 du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique
[27] Article R 161-58 du Code de la sécurité sociale

G. Dans le cas du DMP

- Sa sécurité sera assurée par des mesures impératives :

  - ☛ d'identification et d'authentification des professionnels de santé, décrites ci-dessus,
  - ☛ d'identification par l'INS et d'authentification des patients.
  - ☛ d'autorisation d'accès des professionnels de santé, accordées par le patient, et fonction des habilitations reconnues pour chaque catégorie de professionnels, voire en mode « bris de glace » dans les situations d'urgence ou de risque immédiat,
  - ☛ de journalisation des traces.

III. La dématérialisation des formulaires administratifs

La dématérialisation des formulaires administratifs comporte les avantages suivants :

- un raccourcissement des délais de transmission des formulaires,
- une simplification des démarches administratives.

Dématérialisation de la feuille de soins

- Le principal intérêt de cette dématérialisation réside dans la rapidité du remboursement à l'assuré ou au médecin en cas de tiers payant, ainsi que la sécurisation des flux financiers.
- Le médecin utilise sa carte de professionnel de santé, couplée à la carte Vitale de son patient, afin de créer la feuille de soins électronique (FSE) qui est transmise à l'Assurance-maladie. Un dispositif équivalent à la carte de professionnel de santé pourrait également être utilisé.

Dématérialisation du certificat de décès

- Le médecin peut établir le certificat de décès sur support électronique, après s'être authentifié au moyen de sa carte de professionnel de santé ou d'un système équivalent, afin d'accéder aux formulaires en ligne de certificats de décès[28].
- Cette dématérialisation et la certification électronique permet :

  - ☛ à l'INSERM, aux DDASS et à l'Institut de veille sanitaire de prendre en compte très rapidement les causes médicales de décès à des fins de veille et d'alerte sanitaires,
  - ☛ la confidentialité des données médicales grâce à leur chiffrement.

En exercice libéral, les certificats de décès sont établis au domicile ou au lieu de constatation du décès ce qui limite l'usage de ce procédé électronique.

[28] Arrêté du 24 novembre 2006 modifiant l'arrêté du 24 décembre 1996 relatif aux deux modèles du certificat de décès

Les télé services de l'Assurance-maladie

- L'Assurance-maladie met progressivement en œuvre une série de services se traduisant par la dématérialisation de formulaires et l'accès à des bases de données dans l'objectif non seulement de faciliter l'organisation de l'exercice des médecins mais aussi d'améliorer la rapidité d'accès aux droits pour les patients et la gestion de ces droits. Le CNOM s'associe à cette démarche d'intérêt général.

Le CNOM recommande toutefois que l'accès à ces télé-services soit le plus ergonomique et le moins chronophage possible. Cette recommandation impose d'urgence une large concertation sur la configuration informatique du poste de travail du professionnel afin que les applications qui s'y trouvent et celles qui vont être recherchée en ligne soient compatibles entre elles. La dématérialisation doit en effet permettre impérativement de dégager du temps proprement médical en soulageant le médecin, notamment de premier recours, de ses tâches administratives.

- Ces télé services concernent les professionnels de santé en ambulatoire comme le monde hospitalier.

- Ils portent sur :

  - ☛ l'arrêt de travail
  - ☛ le protocole de soins
  - ☛ la demande d'accord préalable
  - ☛ les certificats médicaux en accident du travail ou maladie professionnelle
  - ☛ la gestion des gardes et astreintes, etc.

- Les formulaires électroniques peuvent être remplis via un simple navigateur web, sous réserve d'avoir installé les kits de gestion des cartes CPS et Vitale adéquats.

- Le médecin s'authentifie sur le site de l'Assurance-maladie grâce à sa carte de professionnel de santé, ou un dispositif équivalent. Il doit également utiliser la carte Vitale de son patient pour l'accès à des bases de données le concernant (historique des remboursements, protocole de soins, notamment).

- Dans le cas du protocole de soins, la dématérialisation vise à faciliter la rédaction du formulaire dans la mesure où les renseignements administratifs sont automatiquement inscrits. Elle permettrait ainsi de gagner du temps dans la procédure d'acceptation par le médecin-conseil du protocole d'exonération du ticket modérateur.

En conclusion

Nous rappellerons un propos de Marie-Anne Frison-Roche [in : *Secrets professionnels. Editions Autrement, Paris, 1999*] : *« le sort du secret professionnel renvoie en effet à des interrogations inquiètes plus générales […] sur l'évolution de nos sociétés : celles-ci après avoir proprement inventé le secret, seraient aujourd'hui submergées par une technique, une technicité et une technicisation qu'elles adorent. Elles y sacrifient – en toute inconscience car la perspicacité technique s'accompagne d'un aveuglement éthique – les libertés des individus qui auraient pu s'épanouir en son sein et qui perdent eux-mêmes concomitamment cette prétention »*

C'est pourquoi ce risque doit être connu, identifié, combattu. Mais on ne saurait dire que, puisque le risque existe, les progrès technologiques seraient redoutables …

A cet égard, la Convention constitutive de l'ASIP santé, agréée par arrêté ministériel, porte la constitution d'un **Conseil d'éthique et de déontologie.** Cela témoigne de l'importance accordée par l'ensemble des acteurs des systèmes d'information partagés de santé aux principes de protection des données de santé à caractère personnel sur lesquels la CNIL exerce déjà sa vigilance.

Ce Conseil d'éthique et de déontologie de l'ASIP santé, qui fait une large place à des représentants très divers mais hautement qualifiés du monde institutionnel et de la société civile, sera présidé par le représentant du CNOM.

Aux côtés de la CNIL et des associations de patients, cela symbolise la place reconnue à l'Ordre national des médecins dans l'organisation des réflexions et des travaux sur les aspects éthiques et déontologiques attachés à « l'informatisation de la santé », à la mise en œuvre prochaine de la télémédecine, aux divers projets et services dont l'ASIP Santé assure la maîtrise d'ouvrage.

Le cadre de vigilance éthique, auquel notre société reste globalement très attachée, prend forme progressivement dans l'espace numérique de la santé et concourt à la construction de l'espace de confiance indispensable au développement de l'e-santé.

Cette construction doit cependant être encore renforcée par des dispositions complémentaires relatives à la sécurité des systèmes d'information de santé. Ces sécurités ne sont pas seulement relatives aux aspects éthiques et déontologiques. La sécurité exige aussi disponibilité, robustesse, résistance aux forces de la cybercriminalité…

De nouveaux textes sont annoncés, visant à consolider le processus d'agrément des hébergeurs de données de santé, et à adapter les systèmes d'authentification des professionnels de santé. La mise en place des répertoires et référentiels devrait, par ailleurs, être accélérée.

Le CNOM restera particulièrement attentif à ces évolutions. Il le sera également vis-à-vis des nouveaux outils et modalités de communication qui apparaissent déjà. Ils pourront tous justifier une adaptation constante de l'implication concrète de l'Ordre dans un monde qui change de plus en plus vite. Ce rapport n'aura été ainsi qu'un rapport d'étape … et cette conclusion temporaire.

Glossaire

- Authentification / identification : l'authentification a pour but de vérifier l'identité dont une entité, un utilisateur de système d'information, se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. S'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité. Dans le monde de la santé, l'authentification est réalisable à l'aide de la carte de professionnel de santé assortie d'un code PIN.

- Autorité de certification (AC) : elle a pour mission, après vérification de l'identité du demandeur du certificat par une autorité d'enregistrement, de signer, d'émettre et de maintenir les certificats électroniques et les listes de révocation. Dans le secteur de la santé, ce rôle est assuré par l'ASIP Santé.

- Autorité d'enregistrement : le décret dit « RPPS » (n° 2009-134 du 6 février 2009, relatif aux procédures liées à l'exercice des professionnels de santé) fixe le cadre réglementaire de la simplification administrative qui fait de l'Ordre le guichet unique de référence (autorité d'enregistrement) pour les professionnels de santé quel que soit leur mode d'exercice (libéral ou salarié).

- Certificat : message électronique écrit suivant une syntaxe définie (format : X.509) et signé par une autorité pour en garantir l'intégrité et la véracité des informations. Il contient l'identité du porteur de certificat, sa clé publique, la durée de vie du certificat, l'identité et la signature de l'AC qui l'a émis.

- Chiffrement : opération par laquelle une donnée intelligible est rendue inintelligible afin d'en protéger la confidentialité.

- Horodatage : service qui associe de manière sûre un évènement et une heure afin d'établir de manière fiable l'heure à laquelle cet évènement s'est réalisé.

- IGC (Infrastructure de gestion de clés), ou PKI (Public Key Infrastructure) : ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs ; l'IGC assure le renouvellement et la révocation des certificats, la publication des certificats valides ou révoqués.

- INS : Identifiant National de Santé, attribué à chaque bénéficiaire de l'assurance maladie, « pour la conservation, l'hébergement et la transmission des informations de santé. Il est également utilisé pour l'ouverture et la tenue du dossier médical personnel et du dossier pharmaceutique » (article L1111-8-1 du CSP).

- Journalisation : action de relever dans un journal tous les évènements qui se produisent dans un système informatique pendant son fonctionnement.

- RPPS : Répertoire Partagé des Professionnels de Santé. Référentiel de données certifiées attachées à un identifiant unique et pérenne du professionnel de santé.

- Traitement de données à caractère personnel : Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction[29].

Avec le Portail de la Sécurité informatique www.securite-informatique.gouv.fr
Et les sites www.gip-cps.fr et www.asipsante.fr.

[29] Article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés