Projet

Arrêté du jj/mm/aaaa pris en application de l'article R.1110-1 du code de la santé publique portant création d'un référentiel relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique.

Version 1.0 du 1 juillet 2008

La ministre de la santé, de la jeunesse, des sports et de la vie associative,

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;
Vu le code de la santé publique, notamment son article R.1110-1 ;
Vu le code de la consommation, notamment son article L.111-1 ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du jj/mm/aaaa ;

Arrête :

Art. 1er. - Aux fins du présent arrêté, on entend par « entité » tout professionnel de santé exerçant à titre libéral, tout établissement de santé, tout réseau de santé ou tout autre organisme délivrant des prestations médicales, qui utilise des moyens électroniques pour effectuer des traitements sur des informations médicales à caractère personnel concernant les personnes qu'il prend en charge.

En application de l'article R.1110-1 du code de la santé publique, il est créé un référentiel dont les exigences sont mentionnées à l'annexe du présent arrêté.

Ce référentiel ainsi que les dispositions du présent arrêté s'imposent aux professionnels de santé exerçant à titre libéral, aux établissements de santé, aux réseaux de santé et aux autres organismes délivrant des prestations médicales, dès lors qu'ils utilisent des moyens électroniques pour effectuer des traitements sur des informations médicales à caractère personnel concernant les personnes qu'ils prennent en charge.

Art. 2. - L'entité met en œuvre une organisation, une politique et des procédures visant à garantir la confidentialité des informations médicales à caractère personnel qu'elle conserve ou transmet.

Cette organisation, cette politique et ces procédures reposent sur l'identification, l'analyse et la gestion des risques d'accès, d'utilisation ou de communication illicites qui peuvent raisonnablement être pris en compte par l'entité.

Pour la mise en œuvre des procédures mentionnées au premier alinéa du présent article, l'entité doit utiliser un système informatique qui respecte les exigences fonctionnelles figurant à l'annexe du présent arrêté. Lorsqu'elle acquiert un produit ou souscrit à un service, l'entité doit vérifier que la documentation commerciale fournie par le vendeur ou le prestataire mentionne, s'il y a lieu, le degré de conformité à tout ou partie de ces exigences fonctionnelles.

Art. 3. - Le directeur général de la santé, le directeur de la sécurité sociale, la directrice de l'hospitalisation et de l'organisation des soins et le secrétaire général des ministères chargés des affaires sociales sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Annexe : Liste des exigences fonctionnelles de sécurité relatives au système informatique.

La présente annexe exprime, sous forme de règles, les exigences fonctionnelles s'appliquant au système informatique utilisé par l'entité.

Différents niveaux de préconisation sont associés à ces règles :

- OBLIGATOIRE : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue ;
- RECOMMANDÉ : ce niveau de préconisation signifie qu'il peut exister des raisons valables dans des circonstances particulières, pour ignorer la règle édictée. Les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;
- CONSEILLÉ : ce niveau de préconisation signifie qu'il est conseillé de suivre la règle édictée si elle présente, pour l'entité, un caractère raisonnable et appropriée.

1.	**GESTION DU CONSENTEMENT DU PATIENT**
1.1.	**Enregistrement du consentement du patient**
1.1.1.	RECOMMANDÉ : Le système permet d'enregistrer les autorisations et interdictions exprimées par le patient relatives à la collecte, à l'accès, au traitement et à la divulgation des informations médicales à caractère personnel le concernant, conformément aux politique et procédures de protection de la confidentialité de l'entité.
2.	**CONTROLE DE L'ACCES AUX INFORMATIONS MEDICALES ET AUX RESSOURCES CRITIQUES**
2.1.	**Protection de l'accès aux informations médicales et aux ressources critiques (i.e., ressources matérielles ou logicielles identifiées comme essentielles pour la protection de la confidentialité des informations médicales à caractère personnel)**
2.1.1.	OBLIGATOIRE : Le système n'autorise l'accès aux informations médicales à caractère personnel et leur traitement (comme : visualisation, création, modification, validation, suppression, impression, transmission ...) qu'aux utilisateurs, applications agissant pour le compte d'utilisateurs, ou groupes d'utilisateurs autorisés, conformément aux politique et procédures de protection de la confidentialité de l'entité.
2.1.2.	OBLIGATOIRE : Le système n'autorise l'accès aux ressources critiques et leur traitement qu'aux utilisateurs, applications agissant pour le compte d'utilisateurs, ou groupes d'utilisateurs autorisés, conformément aux politique et procédures de protection de la confidentialité de l'entité.
2.1.3.	RECOMMANDÉ : Le système supporte des mécanismes d'exception pour déroger aux autorisations d'accès dans des situations particulières motivées, conformément aux politique et procédures de protection de la confidentialité de l'entité. Par exemple, il peut permettre à certains utilisateurs d'accéder, en cas d'urgence, en mode "bris de glace", à des données normalement protégées. L'intégralité des traitements réalisés ainsi que les raisons pour lesquelles ces mécanismes d'exception ont été activés doivent alors être enregistrées pour permettre d'éventuels contrôles ultérieurs.
2.2.	**Gestion des droits d'accès**
2.2.1.	OBLIGATOIRE : Le système permet à des personnes dûment autorisées d'attribuer ou de modifier les droits d'accès accordés à des utilisateurs ou à des groupes d'utilisateurs. Ces droits d'accès précisent notamment la nature des traitements autorisés.

2.2.2.	OBLIGATOIRE : Le système permet d'attribuer les droits d'accès à un utilisateur selon l'un au moins des modèles de contrôle d'accès suivants : 1. L'identité de l'utilisateur ; 2. Le ou les rôles affectés à l'utilisateur au sein de l'entité ; 3. Le contexte d'accès (les droits d'accès sont alors fonction du rôle attribué à l'utilisateur et d'un ensemble d'éléments contextuels : plages horaires, localisation du poste de travail, situations exceptionnelles, exécutions préalables d'actions conditionnelles ...).
2.2.3.	CONSEILLÉ : Le système permet d'attribuer à un utilisateur des droits d'accès ne permettant que la consultation des informations, à des fins d'audit, d'enquête ou de contrôle.
2.2.4.	CONSEILLÉ : Le système permet de supprimer les droits d'accès d'un utilisateur, tout en conservant l'historique des actions et des droits d'accès de cet utilisateur.
2.3.	**Contrôle des droits d'accès**
2.3.1.	RECOMMANDÉ : Le système permet de gérer efficacement les droits d'accès attribués, et notamment de vérifier que les droits d'accès et la manière dont les utilisateurs ont usé de ces droits sont conformes aux politique et procédures de la protection de confidentialité de l'entité.
3.	**AUTHENTIFICATION DES UTILISATEURS ACCEDANT AUX INFORMATIONS MEDICALES OU AUX RESSOURCES CRITIQUES**
3.1.	**Identifiant unique**
3.1.1.	CONSEILLÉ : Le système permet d'attribuer un identifiant unique et exclusif à tout utilisateur autorisé à accéder à des informations médicales à caractère personnel ou à des ressources critiques.
3.2.	**Authentification des utilisateurs**
3.2.1.	OBLIGATOIRE : Le système authentifie les utilisateurs avant tout accès à des informations médicales à caractère personnel ou des ressources critiques.
3.2.2.	RECOMMANDÉ : Le système supporte une technique d'authentification permettant de vérifier l'identité dont se réclame l'utilisateur. Il est conseillé de se référer notamment aux règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard de la DCSSI (www.ssi.gouv.fr).
3.2.3.	RECOMMANDÉ : Le système permet de mettre en œuvre une technique d'authentification à deux facteurs, reposant sur la Carte de Professionnel de Santé.
3.3.	**Sécurité de l'authentification**
3.3.1.	RECOMMANDÉ : Lors des procédures d'authentification, le système ne divulgue que le minimum d'information possible.
3.3.2.	RECOMMANDÉ : Lors de la procédure d'authentification, le système permet d'afficher une mention précisant que l'accès au système est réservé aux seuls utilisateurs autorisés. Il informe les utilisateurs autorisés du caractère confidentiel des informations.
3.3.3.	RECOMMANDÉ : Le système permet de définir le nombre maximal de tentatives successives infructueuses de connexions au delà duquel le compte utilisateur est bloqué temporairement ou nécessite l'intervention d'un administrateur.

3.3.4.	OBLIGATOIRE : Le système permet de détecter l'inactivité des sessions ouvertes par les utilisateurs. Il permet de les fermer ou de les verrouiller automatiquement après un délai paramétrable. La fermeture ou le verrouillage manuel sont également possibles.
3.3.5.	OBLIGATOIRE : Lorsque l'authentification des utilisateurs est réalisée sur la base d'un mot de passe, le système supporte des dispositifs en assurant l'efficacité. Par exemple : - il permet d'imposer des règles relatives à la force des mots de passe (comme : longueur minimale, utilisation conjointe de chiffres, lettres, majuscules, minuscules, caractères spéciaux …) ; - il permet aux utilisateurs de changer eux-mêmes leur mot de passe ; - il permet à certains utilisateurs dûment habilités de réinitialiser les mots de passe ; - il permet d'imposer aux utilisateurs dont le mot de passe a été réinitialisé par un tiers de changer leur mot de passe à la connexion suivante ; - il supporte les caractères alphanumériques et spéciaux du jeu de caractères ASCII ; - il permet d'imposer aux utilisateurs de modifier périodiquement leur mot de passe, sans pouvoir réutiliser les précédents ; - il ne transporte ni ne stocke en clair les mots de passe. Il les protège en utilisant des algorithmes de chiffrement ou de hachage comme 3DES, AES, SHA1 ou leurs successeurs.
3.3.6	RECOMMANDÉ : Lorsque la Carte de Professionnel de Santé est utilisée, le système permet de fermer automatiquement, au retrait de la carte, la session ouverte par l'utilisateur**.**
3.3.7	RECOMMANDÉ : Lorsque la Carte de Professionnel de Santé est utilisée, le système doit vérifier que la carte n'est pas mise en opposition, en se référant à la dernière liste des certificats révoqués publiée par le GIP CPS.
3.3.8	RECOMMANDÉ : Lorsque la Carte de Professionnel est utilisée, le système doit contrôler la date de fin de validité de la carte et la validité des certificats que la carte contient, notamment en vérifiant le chemin de certification jusqu'au certificat racine du GIP CPS.
4.	**AUDITABILITE DE L'ACCES AUX INFORMATIONS MEDICALES ET AUX RESSOURCES CRITIQUES**
4.1.	**Détection des évènements**
4.1.1.	CONSEILLÉ : Le système détecte en temps réel les évènements le concernant et qui peuvent affecter la confidentialité des informations médicales à caractère personnel.
4.2.	**Enregistrement des traces**
4.2.1.	CONSEILLÉ : Le système permet d'enregistrer une trace des évènements pouvant affecter la confidentialité des informations médicales à caractère personnel dans des journaux d'audit. Ces évènements sont, au minimum, les suivants : lancement/arrêt du système, tentative réussie/rejetée de connexion des utilisateurs, déconnexion des utilisateurs, expiration des connexions, verrouillage des comptes utilisateurs, création/consultation/mise à jour/suppression de informations médicales à caractère personnel, import/export, transmission/réception de informations médicales à caractère personnel, évènement relatif aux fonctions d'administration de la sécurité, et notamment de gestion des droits d'accès.
4.2.2.	RECOMMANDÉ : Le système permet d'enregistrer une trace de tous les traitements d'informations médicales à caractère personnel (comme : consultation, création, modification, validation, impression, copie, import, export, transmission, réception …) avec l'identifiant de l'utilisateur - ou de l'application agissant pour le compte d'utilisateur - ayant effectué ces traitements, et, le cas échéant, l'identifiant de la personne pour le compte de laquelle ces opérations ont été effectuées. Le système est capable d'y associer les informations médicales à caractère personnel sur lesquelles ces opérations ont porté.

4.2.3.	RECOMMANDÉ : Le système permet aux personnes dûment autorisées d'activer ou désactiver la journalisation de certains évènements, conformément aux politique et procédures de protection de la confidentialité de l'entité.
4.3.	**Contenu des traces**
4.3.1.	CONSEILLÉ : Pour chacun des évènements figurant dans les journaux d'audit, le système permet d'enregistrer, lorsqu'ils sont pertinents, les éléments suivants : date/heure de l'évènement, composant du système concerné, type d'évènement, identifiant de l'utilisateur ou référence du système déclenchant l'évènement, description des informations médicales à caractère personnel et identifiant du patient concerné, résultat de l'évènement.
4.3.2.	RECOMMANDÉ : Pour chaque traitement d'informations médicales à caractère personnel ayant donné lieu à enregistrement de trace, le système permet d'enregistrer l'identifiant de l'utilisateur ayant effectué ces traitements, et, le cas échéant, l'identifiant de la personne pour le compte de laquelle ces opérations ont été effectuées. Le système permet d'y associer les informations médicales à caractère personnel sur lesquelles ces opérations ont porté.
4.3.3.	RECOMMANDÉ : En cas de transmission d'informations médicales à caractère personnel, ou d'accès à ces informations par des personnes extérieures à l'entité, le système permet de conserver des informations relatives au contexte de la transmission ou d'accès, comme l'origine et la destination des informations médicales.
4.3.4.	CONSEILLÉ : Le système est capable de se baser sur l'échelle de temps UTC pour horodater les évènements relatifs à la confidentialité des informations médicales à caractère personnel.
4.4.	**Exploitation des traces**
4.4.1.	RECOMMANDÉ : Le système permet d'accéder à toutes les informations contenues dans les journaux d'audit. Le système permet d'exploiter les journaux d'audit, notamment pour vérifier que les politique et procédures de protection de la confidentialité de l'entité ont été respectées, soit directement, en supportant des fonctions de gestion, de surveillance et d'analyse de ces journaux, soit indirectement, en permettant d'exporter les journaux.
4.4.2.	RECOMMANDÉ : Le système permet de reconstituer aisément l'historique des accès et des traitements relatif au dossier médical d'un patient donné, en y associant dates et heures d'accès.
4.4.3	CONSEILLÉ : Le système permet de reconstituer aisément la liste des patients aux informations desquels un utilisateur donné a accédé, en y associant dates et heures d'accès.
4.5.	**Protection des traces**
4.5.1.	RECOMMANDÉ : Le système n'autorise l'accès aux journaux d'audit qu'aux personnes dûment autorisées - ou aux applications agissant pour le compte de telles personnes.
4.5.2.	RECOMMANDÉ : Le système est capable de détecter toute modification des journaux d'audit.
4.5.3.	RECOMMANDÉ : Les journaux d'audit doivent pouvoir être sauvegardés, restaurés et archivés.
4.5.4.	CONSEILLÉ : Les sauvegardes et archives des journaux d'audit doivent pouvoir présenter un niveau de protection au moins équivalent à celui visé lors de la constitution des journaux d'audit.
5.	**TRANSMISSION D'INFORMATION MEDICALES SUR UN RESEAU OUVERT**

5.1.	**Chiffrement des données**
5.1.1.	OBLIGATOIRE : Si le système échange des informations médicales à caractère personnel sur internet ou tout autre réseau ouvert, il permet de les chiffrer conformément à l'état de l'art. Il recourt à un algorithme comme 3-DES, AES ou à tout autre algorithme au moins équivalent en terme de robustesse, associé, de préférence, à un standard ouvert (comme SSL, TLS, IPsec, XML encryption, S/MIME, ou équivalents et successeurs). Il est conseillé de se référer, pour toute information sur les algorithmes, longueurs de clés et modes opératoires, aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard de la DCSSI (www.ssi.gouv.fr).
5.1.2	OBLIGATOIRE : Si le système échange des informations médicales à caractère personnel sur internet et les chiffre en utilisant le standard S/MIME, il recourt aux certificats délivrés par le GIP CPS.
5.1.3	RECOMMANDÉ : Si le système permet d'échanger des informations médicales à caractère personnel sur internet avec des professionnels de santé, il permet d'échanger des messages chiffrés en utilisant le standard S/MIME et en recourant aux certificats délivrés par le GIP CPS.
5.2.	**Authentification des parties**
5.2.1.	OBLIGATOIRE : Si le système échange des informations médicales à caractère personnel sur internet ou tout autre réseau ouvert, il permet d'authentifier le destinataire ou l'entité destinataire en ayant recours, de préférence, à un standard ouvert d'authentification mutuelle (par exemple : SSL, TLS, IPsec, XML sig, S/MIME, ou équivalents et successeurs). L'authentification peut néanmoins être assurée en recourant à des mesures non techniques, notamment organisationnelles, conformément aux politique et procédures de protection de la confidentialité de l'entité.
5.2.2	OBLIGATOIRE : Si le système échange des informations médicales à caractère personnel sur internet et authentifie le destinataire en utilisant le standard S/MIME, il recourt aux certificats délivrés par le GIP CPS.
6.	**EXPLOITATION DU SYSTEME**
6.1.	**Sauvegarde et archivage**
6.1.1.	RECOMMANDÉ : Le système permet d'inactiver, d'archiver, de restaurer et de détruire les informations médicales à caractère personnel, conformément aux politiques et procédures de protection de la confidentialité de l'entité.
6.1.2.	RECOMMANDÉ : Les informations médicales à caractère personnel, lorsqu'elles sont sauvegardées à des fins de continuité d'activité ou archivées, doivent avoir un niveau de protection au moins équivalent aux informations médicales à caractère personnel d'utilisation courante.
6.1.3.	RECOMMANDÉ : Les informations médicales à caractère personnel, lorsqu'elles sont archivées, doivent pouvoir être chiffrées, pseudonymisées ou anonymisées.
6.1.4.	RECOMMANDÉ : Les supports (disques durs …) contenant des informations médicales à caractère personnel doivent pouvoir être détruits ou réinitialisés en fonction du niveau de confidentialité de ces données. Il est conseillé de se référer notamment au guide technique pour la confidentialité des disques durs à recycler ou à exporter de la DCSSI (www.ssi.gouv.fr).
6.2.	**Dispositifs portables**

6.2.1.	OBLIGATOIRE : Si le système stocke des informations médicales à caractère personnel sur des dispositifs portables (ordinateur portable, clé USB, CD ou DVD, smartphone, PDA …), ces informations doivent pouvoir être chiffrées en utilisant des algorithmes comme 3-DES, AES ou leurs successeurs. Il est conseillé de se référer, pour toute information sur les algorithmes, longueurs de clés et modes opératoires, aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard de la DCSSI (www.ssi.gouv.fr).
6.3.	**Protection contre les codes malveillants**
6.3.1.	OBLIGATOIRE : S'il est connecté à internet ou à tout autre réseau ouvert, le système utilisé doit comporter des dispositifs de détection, de prévention et de neutralisation des codes malveillants, conformes à l'état de l'art.
6.4.	**Sécurité des services réseau**
6.4.1.	OBLIGATOIRE : S'il est connecté à internet ou à tout autre réseau ouvert, le système doit pouvoir être configuré de façon à ne permettre que les services et protocoles réseaux strictement nécessaires.
7.	**DOCUMENTATION**
7.1.	**Qualité de la documentation**
7.1.1.	CONSEILLÉ : Les fonctions de sécurité du système sont décrites dans un langage compréhensible par les administrateurs et utilisateurs du système, de manière à permettre une installation, une exploitation et une utilisation sûres. Les messages d'erreurs ou d'alertes sont décrits de façon claire et explicite et sont associés à des propositions d'actions correctives.