Union régionale des caisses d'assurance maladie
Provence Alpes Côte d'Azur

Agence régionale de l'hospitalisation
Provence Alpes Côte d'Azur

Guide
sur la sécurité
des échanges informatisés
d'informations médicales

Novembre 2003

urcam

Intention

Ce document a pour objectif de rappeler les principes de la sécurité informatique, d 'informer les promoteurs de projet mettant en oeuvre un échange ou un partage d' informations médicales individualisées de l'état de l'art dans ce domaine ainsi que des contraintes légales qui s'appliquent à leur activité professionnelle. Ceci doit leur permettre de mieux exprimer leur demande auprès de leur prestataire informatique, et donc de mieux analyser l'offre de celui-ci. De même cela doit leur permettre de comprendre les exigences des partenaires institutionnels en ce qui concerne la sécurité des données gérées par leur projet.

Introduction

Comme tous les secteurs professionnels, le secteur de la santé connaît depuis dix ans une évolution de ses pratiques liée à l'informatisation progressive des différents acteurs.

La carte Vitale représente l'innovation la plus connue du grand public, mais le mouvement va bien au-delà du seul remboursement des soins aux assurés, et englobe aussi bien le suivi des dossiers patients que les échanges entre professionnels libéraux ou hospitaliers, les envois de résultats d'analyses ou d'imagerie, la tenue des dossiers administratifs dans les établissements de soins, ou l'accès des professionnels à l'information sur les médicaments ou la recherche.

Ces échanges et ce partage des données, portant souvent sur des informations nominatives et confidentielles concernant les patients, et engageant la responsabilité de leur auteur (analyses, diagnostics), doivent bien sûr présenter toutes les garanties de sécurité sans lesquelles la confiance ne pourrait s'établir.

Les contraintes sécuritaires

La loi et la déontologie imposent des contraintes fortes lors de l'utilisation des nouvelles technologies dans le secteur de la santé. Ces contraintes permettent de fonder la confiance que les acteurs peuvent s'accorder entre eux, et qu'ils peuvent accorder au système.

La première de ces contraintes, inscrite dans le code de la santé publique depuis **la loi du 4 mars 2002**, est la confidentialité des données concernant les patients, aussi bien lors d'un échange ponctuel entre confrères, qu'à l'occasion de la mise sur serveur de dossiers ou de parties de dossier : les données doivent être protégées pour éviter toute lecture par des personnes non autorisées. Toute demande devra être conforme à la réglementation en vigueur sur les hébergeurs de données médicales.

Un premier niveau de sécurité concerne **le contrôle de l'accès physique** aux matériels : par exemple, comment on accède à l'ordinateur d'un cabinet ou au serveur d'une structure, comment on démarre ces systèmes... C'est souvent un aspect négligé qui doit recueillir autant d'attention que les dossiers-papiers confidentiels laissés sur les bureaux. S'il s'agit de communiquer un flux d'information nominatives, ou indirectement nominatives (ex. mail, fichier joint...), il faudra alors le **chiffrer**. Pour les données stockées sur un serveur, seuls les professionnels authentifiés en charge du traitement du patient et autorisés par celui-ci devront pouvoir accéder à ces informations, et, si le dossier est complet, ils doivent ne pouvoir accéder qu'aux seules informations pour lesquelles ils sont autorisés. Ces restrictions nécessitent la mise en place d'une **authentification *personnelle*** de chaque intervenant et une **habilitation de l'application**. Notons que la loi prévoit que le **patient** soit à même de déclarer qui a accès à ses données.

Certains types d'informations doivent également être protégés de manière générale en s'assurant de la qualité du professionnel de santé, mais sans avoir besoin nécessairement de son nom. Une **authentification *professionnelle*** est alors nécessaire. La sécurité du patient exige que l'on puisse s'assurer de **l'intégrité des données** le concernant (penser à des résultats d'analyse ou à des prescriptions, pour lesquels toute modification intentionnelle ou non peut avoir des conséquences graves) et de la responsabilité de celui qui les a écrites. Ces garanties relèvent de la signature électronique, telle qu'elle a été reconnue par **la loi du 13 mars 2000**.

Dans le cas de données stockées sur serveur permettant un accès partagé, il est utile de savoir qui a accédé à telle information et qui a modifié telle autre : cette **traçabilité** requiert la tenue, par l'application, d'un journal des accès et des modifications. La signature électronique sur les données modifiées peut aussi être utilisée dans ce cadre.

Enfin il faut garantir l'accessibilité et la **conservation des informations** stockées sur serveur : un dossier perdu ou inaccessible ne sert à rien. Les responsables informatiques doivent veiller à la sauvegarde des disques, et à la redondance et au dimensionnement de leurs infrastructures, pour garantir la continuité et la pérennité de l'accès.
Nous mentionnerons également pour mémoire la nécessité absolue de disposer de **logiciels pare-feu et anti-virus** régulièrement mis à jour. De même, le promoteur du projet doit signer avec son prestataire informatique un **accord de confidentialité** extrêmement strict vis à vis de ses interventions sur les applications gérant des don-

nées confidentielles, ainsi qu'un **contrat de suivi logiciel** et un **contrat de maintenance matérielle** permettant au promoteur du projet d'éviter les risques de sécurité liés à des bugs ou à des défauts matériels de son équipement.

En résumé, les fonctionnalités indispensables pour fonder la confiance des professionnels de la santé dans les échanges et le partage de données médicales sont principalement :

Les besoins de sécurité	Les solutions
1. La confidentialité des informations	Le contrôle d'accès et le chiffrement
2. L'authentification des personnes et des qualités	La présentation à l'autre d'une preuve infalsifiable et vérifiable de son identité et de sa qualité de professionnel de santé (ex. ordonnance-papier signée carte plastifiée de l'Ordre CPS en tant que carte d'identité professionnelle électronique)
3. L'intégrité des données	La signature électronique qui par son mécanisme garantit que le message n'a pas été altéré ou modifié.
4. L'engagement la preuve de l'engagement	La signature électronique au même titre que la signature manuscrite
5. La traçabilité des données	La journalisation des accès et des modifications la signature électronique
6. La conservation des données	La sauvegarde régulière des données l'archivage
7. La disponibilité des données	La redondance des équipements le dimensionnement des infrastructures
8. L'utilisation adéquate des fonctions de sécurité	La définition de bonnes pratiques et leur respect

Dans la liste ci-dessus, la fonctionnalité n°8 relève de l'organisation du travail. Il ne sert à rien d'installer une porte blindée avec des verrous multipoints si on laisse la clé dessus. A cet égard, il est également primordial, tant pour un dossier sur serveur que pour un envoi ponctuel, de s'assurer que les informations concernant le patient sont **pertinentes et à jour**. Aucune technologie ne pouvant assurer cela, il faut s'en remettre aux bonnes pratiques des intervenants.

Les fonctionnalités 5, 6 et 7 sont du domaine de l'administration et de l'exploitation informatiques classiques. En revanche les quatre premières fonctionnalités, telles qu'elles sont assurées aujourd'hui par le système CPS, correspondent au niveau d'exigence attendu par les partenaires institutionnels. Une solution unique intégrant les 4 fonctions est préférable à des solutions distinctes, avec un niveau de sécurité au moins équivalent à celui d'un système à carte à puce.

Le GIP "CPS", qui rassemble tous les acteurs du secteur santé social (Etat, CNAM, Ordres et syndicats professionnels...), a reçu pour mission de concevoir, d'émettre et de promouvoir un système garantissant la sécurité des échanges et du partage des données médicales. Le système CPS, basé sur les technologies standards les plus avancées, apporte à tous les utilisateurs les garanties dont ils ont besoin concernant les fonctionnalités 1 à 4 citées ci-dessus. Il permet une compatibilité complète de **tous** les professionnels du secteur, quels que soient les fournisseurs d'accès internet, les environnements informatiques, les systèmes d'information utilisés.

Au-delà de ces fonctionnalités liées à la sécurité informatique, il serait souhaitable de favoriser un système qui assure la pérennité de la solution de sécurité dans le temps et qui permette un élargissement sans avoir à redévelopper les outils.

Annexe

Les apports du système CPS

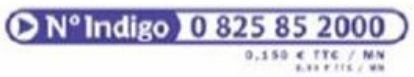
La carte CPS contient les certificats et les clés nécessaires à son porteur...

Pour :	Et répondre aux questions :
Garantir son identité et sa qualité	Comment être sûr de l'identité de l'émetteur d'un message ?
Signer électroniquement (au sens de la loi sur la signature électronique) ses mails ou ses documents et en garantir l'intégrité	Comment éviter les altérations de données lors de l'échange ? Comment s'assurer de son engagement sur le contenu du message ?
Chiffrer des informations pour les rendre confidentielles	Comment assurer la confidentialité de l'échange ?
S'authentifier pour accéder, de manière confidentielle, à des systèmes d'informations ou à des serveurs web réservés.	Comment, pour l'utilisateur, être sûr de l'authenticité du serveur (éviter les imposteurs) ?Comment, pour le serveur, être sûr de l'authenticité de l'utilisateur (pour lui ouvrir des droits) ?

La CPS constitue donc à la fois une « carte d'identité professionnelle électronique » et un « sceau électronique », mais cela ne présume en rien de l'usage qui en sera fait. Il revient aux applications mettant en oeuvre ses fonctionnalités de s'en servir à bon escient. Il revient aux développeurs d'applications et aux éditeurs de logiciels d'intégrer systématiquement l'usage de la CPS dans les applications et systèmes d'informations du secteur de la santé, pour gérer le filtrage des accès, la gestion des droits des intervenants, la traçabilité des actions, etc.

L'offre de services du GIP "CPS" comporte également un **annuaire des porteurs de certificats**, ainsi qu'une liste des certificats révoqués (pour pouvoir vérifier la validité d'une carte ou d'un certificat).

Un **centre d'appels** répond aux questions des utilisateurs 7 jours sur 7 de 8h30 à 22h (24h/24 pour enregistrer les pertes ou vols de cartes) :



Un **site web** (http://www.gip-cps.fr) apporte de nombreuses informations utiles (les cartes, le système CPS, les aspects juridiques...).

L'intégration du système CPS

Pour pouvoir intégrer la CPS dans une application, il est nécessaire d'obtenir pour votre projet l'avis favorable du **Collège de Déontologie** du GIP "CPS", qui se prononce sur les aspects déontologiques et juridiques. Pour les intégrateurs, le GIP "CPS" propose **un kit et un manuel d'intégration**, des **cartes de tests** et des **formations.**

Pour ces deux actions, veuillez vous adresser au Service Relations Extérieures du GIP CPS, 8 bis rue de Châteaudun, 75009 Paris (Tél. : 01 44 53 36 48, Fax : 01 44 53 33 25) qui vous communiquera les documents nécessaires à la préparation de votre demande.

Pour équiper ensuite les membres d'un projet en cartes de la famille CPS, voici les démarches à suivre :

<table>
<tr><th>Activité principale en :</th><th>Établissement</th><th>Libéral</th></tr>
<tr><td>CPS pour les professionnels de santé
  </td><td rowspan="3">L'obtention des cartes dans un établissement est subordonnée à la demande de la carte du directeur de l'établissement (CDE).

Vous pouvez accéder à la procédure de demande pour les directeurs d'établissements ou de demande de salariés depuis le site web du GIP CPS :
www.gip-cps.fr (espace services « devenez utilisateur)
Ou appelez le :
N° Indigo 0 825 85 2000
0,150 € TTC / MN</td><td>Contactez votre Ordre (ou, par défaut, votre DDASS).
Vous recevrez alors un formulaire pré-renseigné à retourner signé à l'Ordre (ou à la DDASS).</td></tr>
<tr><td>CPF pour les professionnels de santé en formation (ex. internes)
  </td><td>Non applicable</td></tr>
<tr><td>CDE et CPE destinées au personnel des structures de soins, aux établissements de santé, aux laboratoires, aux CPAM, etc.
  </td><td>Le responsable du cabinet fait la demande de CPE pour le personnel de ce cabinet auprès de son Ordre (ou, à défaut, de la DDASS).</td></tr>
<tr><td>CPA pour les personnes employées par des organismes, institutions ou entreprises ayant reçu un accord ministériel (ex. ministère de l'emploi et de la solidarité, GIP CPS, opérateurs de réseau…). Par exemple, le personnel social d'un réseau de santé peut obtenir une carte dans ce cadre.
  </td><td colspan="2">Autres structures
La distribution des cartes CPA au personnel d'un organisme est subordonnée à la délivrance de la carte CPA au responsable de cet organisme. Vous trouverez des renseignements sur le site web du GIP CPS :
www.gip-cps.fr (espace services « devenez utilisateur)
Ou appelez le :
N° Indigo 0 825 85 2000
0,150 € TTC / MN</td></tr>
</table>