La Cybersanté et la sécurité des données médicales

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

Par :

Eléonore SCHAULI

Conseiller au travail de Bachelor :

David BILLARD, professeur à la HEG

Genève, le 24 novembre 2008

Haute École de Gestion de Genève (HEG-GE)

Informatique de Gestion

Déclarations

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre d'informaticienne de gestion. L'étudiante accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG[1].

« J'atteste avoir réalisé seule le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 24 novembre 2008

Eléonore Schauli

1 Haute Ecole de Gestion

Remerciements

Je tiens à remercier :

- Monsieur **David BILLARD**, mon directeur de mémoire, qui m'a aidé à trouver des contacts très précieux pour mes recherches et à suivi régulièrement l'avancement de mon travail.
- Le Professeur **Christian LOVIS**, informaticien au service informatique médical des HUG[2], qui m'a consacré du temps, m'a donné des informations très utiles ainsi que des documents qu'il utilise pour ses cours aux étudiants en informatique médicale.
- Monsieur **Franco SERENA**, responsable de projets informatiques à l'Université de Genève. Concepteur de l'application de gestion administrative des patients de la section de médecine dentaire de l'Université de Genève aux HUG.
- Monsieur **José CAMPOS**, médecin aux HUG en orthopédie.
- Madame **Lisa GAUTSCHI**, infirmière à la FSASD[3].
- Madame **Laurence GROUX**, infirmière aux HUG.

2 Hôpitaux Universitaires de Genève

3 Fondation des Services d'Aide et de Soins à Domicile

Sommaire

J'ai choisi ce sujet pour mon travail de Bachelor car il est vraiment d'actualité et nous concerne tous. De plus, il permettra de comprendre la perspective de la cybersanté[4] suisse.

Une première partie traitera des lois suisses dans le domaine de la santé. Ensuite, un état des lieux de ce qui existe en Suisse ainsi qu'à l'étranger offrira un aperçu des pratiques dans le monde médical et des avantages et des inconvénients des systèmes utilisés. Enfin, un chapitre sur la sécurité expliquera le fonctionnement de la cryptographie et les différents moyens de chiffrement évoqués dans les précédents chapitres.

Dans un premier temps, mon idée était axée sur la sécurité des données médicales; au fil des jours, j'ai constaté que ce point n'était pas le plus important mais que c'était la mise en commun des projets sur la cybersanté qui posait problème et était au cœur du sujet. J'ai donc changé le titre initial qui était **« La sécurité des données médicales »** en **« La Cybersanté et la sécurité des données médicales »**.

Pour réaliser ce mémoire, j'ai effectué d'importantes recherches documentaires à l'aide d'Internet, en restant prudente face à l'infobésité que propose le web. De plus, j'ai dû définir chacun des termes utilisés pendant mes recherches car même les personnes familiarisées avec ce domaine se contredisent les unes des autres.

Pour la recherche documentaire, j'ai dû être très vigilante concernant les informations trouvées sur le net car un grand nombre de sources proviennent d'auteurs inconnus, ce qui ne garantit pas leur fiabilité.

Les sites Internet suisses offrent de nombreuses informations qui souvent ne sont pas traduites en français. J'ai donc dû également faire un travail de traduction.

Un autre aspect délicat à relever a été la tendance qu'ont les gens à franciser le jargon anglophone touchant l'univers informatique et médical. Des appellations différentes étaient données à des projets similaires. Il a fallu structurer les informations et éliminer celles qui étaient identiques pour ne pas me perdre.

4 Service de santé électronique

Dans le cadre de ce travail, j'ai obtenu un rendez-vous avec un informaticien des HUG, le Professeur Christian LOVIS, qui m'a expliqué le système employé à l'hôpital ainsi que ceux utilisés en Suisse. De plus il m'a donné des sources de sites Internet « fiables », c'est-à-dire des sources professionnelles donc sûres. J'ai ensuite rencontré un autre informaticien de l'UNIGE[5], Monsieur Franco SERENA, qui a créé l'application administrative des patients pour la section de médecine dentaire de l'Université de Genève aux HUG. Plusieurs de mes connaissances travaillant dans le domaine de la santé ont aussi bien voulu répondre à mes questions concernant leur point de vue sur la cybersanté et la sécurité des données médicales.

Ces divers contacts m'ont amené à une meilleure compréhension du projet et m'ont permis de me diriger vers des informations fiables concernant mon travail.

Dans ce travail de mémoire, je m'adresse autant à des informaticiens qu'à des personnes du corps médical ou à un public non familiarisé dans ces deux domaines; les mots techniques et les acronymes utilisés sont répertoriés dans un lexique et un glossaire à la fin du document.

Pour conclure, je n'apporte pas de solution mais souhaite dresser un état des lieux de ce qui existe. Il permet de mettre en lumière la manière dont une stratégie de cybersanté et de sécurité des données peut être instaurée. Mon opinion sur le sujet est la suivante : je suis favorable à la mise en place d'une stratégie de cybersanté et la sécurité des données ne m'inquiète pas, pour autant qu'elle soit bien gérée et donc la vigilance est de mise.

5 Université de Genève

« Les ordinateurs ne sont pas fiables, les hommes le sont encore moins. À l'origine de chaque erreur attribuée à l'ordinateur, on trouve au moins deux erreurs humaines, dont celle qui consiste à accuser l'ordinateur. »

Loi de non-fiabilité de Gibbs

Table des matières

Déclarations 2
Remerciements 3
Sommaire 4
Liste des Tableaux 10
Liste des Figures 10
Introduction 12
1. Le secret médical 13
1.1. Violation du secret de fonction 13
1.2. Violation du secret professionnel 13
1.3. Le devoir de discrétion 14
1.4. Serment d'Hippocrate 14
1.5. Ce que dit la loi suisse 15
1.6. Les assurances maladies 16
2. Qu'existe-t-il en Suisse ? 17
2.1. Les TrustCenters 18
2.1.1. Clientèle des TrustCenters 19
2.1.1.1. Ctésias 19
2.1.2. TrustX 20
2.1.2.1. Trois façons de transférer les données : 22
2.1.2.2. Processus de facturation 22
2.1.2.3. Que faut-il pour utiliser TrustX ? 24
2.2. NewIndex 24
2.3. HIN 24
2.3.1. ASAS 26
2.3.2. HIN MailGateway 28
2.4. H-Net 30
2.5. Système Covercard® 31
2.6. Stratégie eHealth 33
2.6.1. Publifocus 35
2.6.2. Objectifs pour le dossier électronique du patient 35
2.6.3. Objectifs pour le service en ligne 37
2.6.4. Service qualité et label 40
2.6.5. Le dossier électronique du patient 43
2.6.6. Dossier patient intégré (DPI) aux HUG 44
2.6.7. Carte d'assuré 48
2.6.7.1. Ordonnance électronique 49
2.6.7.2. Télémédecine 49

2.6.8. Carte professionnelle de santé *49*
2.6.9. Projet e-Toile *50*
2.6.10. Projets dans d'autres cantons *52*
2.6.11. Standards et interopérabilité *52*
2.6.11.1. HL7 52
2.6.11.2. CDA 53
2.6.11.3. DICOM 53
2.6.11.4. CUMUL 53
2.6.11.5. LOINC 54
2.7. Pour ou contre ? 54
3. Qu'existe-t-il à l'étranger ? 56
3.1. VeriChip 56
3.2. Carte Vitale 58
3.2.1. De gros problèmes de sécurité *58*
3.2.2. Carte Vitale 2 ..... *58*
3.3. Google Health 59
3.3.1. Traduction des conditions de Google Health *61*
3.3.2. Autorisation *62*
3.3.3. Centre d'aide Google Health *63*
4. La sécurité des systèmes d'information 64
4.1. Politique de sécurité 64
4.2. Les hackers 65
4.3. Les failles 65
4.3.1. Les erreurs humaines *66*
4.3.1.1. Comment s'en protéger ? 68
4.3.2. Cas de failles *68*
4.4. La cryptographie 70
4.4.1. Exemples de cryptogrammes *70*
4.4.2. Fonction de Hachage *71*
4.4.3. OTP *72*
4.4.4. Chiffrement synchrone *73*
4.4.5. Chiffrement asynchrone *73*
4.4.6. Cryptographie symétrique – à clef privée *73*
4.4.6.1. AES 73
4.4.6.2. SSL 74
4.4.7. Cryptographie asymétrique – à clef publique *74*
4.4.7.1. PKI 74
4.4.7.2. RSA 75
4.5. S/MIME 77

4.6. Single-Sign-On 77
4.7. La signature numérique 78
4.7.1. Norme X.509 78
4.7.2. Textes de loi suisse sur la signature électronique 80
Mise en perspective 83
Conclusion 85
Index 86
Glossaire 90
Bibliographie 97
Annexe 1 Facture Tarmed 102
Annexe 2 Code diagnostics 103
Annexe 3 DATALOSSdb 107
Annexe 4 Profils des droits d'accès du DPI 108

Liste des Tableaux

Tableau 1 Données de clientèle TC (TrustCenter) 19
Tableau 2 Statistiques du nombre de factures dans le miroir du cabinet 20
Tableau 3 Analyse de Google par Privacy International 60
Tableau 4 Incidents entre janvier et juillet 2008 dans le milieu médical 69
Tableau 5 Récapitulatif des projets et systèmes en exploitation 83

Liste des Figures

Figure 1 Hippocrate 15
Figure 2 Le serment d'Hippocrate 15
Figure 3 Ensemble du processus de l'échange des données 21
Figure 4 Anonymisation d'une facture 22
Figure 5 Facturation « aller-chercher » (Tiers Garant) 23
Figure 6 Facturation « apporter » (Tiers Payant) 23
Figure 7 Croissance continue de l'abonnement individuel 25
Figure 8 Plateforme HIN et clients 27
Figure 9 Schéma de topologie HIN Access Control Services 27
Figure 10 Schéma de topologie HIN MailGateway 29
Figure 11 Réseau H-Net 30
Figure 12 Fonctionnement du service PostFinance 31
Figure 13 Carte Covercard® 31
Figure 14 Nombre de porteurs de carte Covercard® 32
Figure 15 Données et codes Covercard® 32
Figure 16 Processus d'échanges de données avec la Covercard® 33
Figure 17 Planning du projet de la stratégie eHealth 34
Figure 18 Planning du dossier électronique du patient 36
Figure 19 Planning du service en ligne 38
Figure 20 Conditions-cadres et accords politiques et légaux 39
Figure 21 Sceau HONcode, preuve de certification 40
Figure 22 Processus de certification 41
Figure 23 Processus de réévaluation 42
Figure 24 Barre d'outils de certification HONcode 42
Figure 25 Générateur de cryptage d'adresses e-mail 43
Figure 26 Carte à puce des employés HUG 45
Figure 27 Page d'accès au Dossier Patient Intégré 45
Figure 28 Demande de droits d'accès 46

Figure 29 Principe de vitre brisée 47
Figure 30 Surveillance d'accès après le principe de vitre brisée 48
Figure 31 HPC 49
Figure 32 Architecture du réseau e-Toile 50
Figure 33 Architecture et exemples 51
Figure 34 Partenaires e-Toile 51
Figure 35 Image de médecine nucléaire au format DICOM 53
Figure 36 Puce électronique VeriChip 57
Figure 37 Lecteur optique 57
Figure 38 Portillon lecteur optique 57
Figure 39 Carte Vitale 2 58
Figure 40 Mon PHR Google Health 59
Figure 41 Pourcentage de failles par secteur 66
Figure 42 Nombre d'incidents par secteur entre janvier et juillet 2008 69
Figure 43 Fréquence moyenne des lettres dans l'alphabet 71
Figure 44 Système d'identification par OTP 72
Figure 45 Cryptographie asymétrique 76
Figure 46 Certificat de norme X.509 79
Figure 47 Certificat Swisscom 79

Introduction

L'objectif de ce travail a pour but de découvrir ce qui existe en matière de cybersanté et de la sécurité qui en découle, d'analyser l'existant et son développement dans le futur.

Dans notre société, l'informatique est devenue incontournable. Le domaine de la santé n'y échappe pas et la sécurité des données médicales constitue un enjeu majeur. En Suisse et à l'étranger de nombreux projets sont à l'étude; on constate à ce jour qu'il est difficile de changer les habitudes des gens, que les coûts de la mise en œuvre des projets constituent un obstacle, enfin que la sensibilité des données ne facilite pas leur réalisation.

Le but d'un système de cybersanté est de permettre l'accès à des données regroupées, mises à jour et fiables. Cependant, les différences linguistiques en Suisse ne facilitent pas la mise en commun de projets informatiques.

Le nombre élevé à ce jour de tels projets et d'idées prouve bien que le domaine médical ne peut plus se passer des technologies de l'information pour améliorer la qualité des soins et en réduire les coûts. L'article 41 de la Constitution fédérale stipule que toute personne en Suisse doit pouvoir bénéficier de soins. La population augmentant, il faut donc penser à améliorer les processus de gestion de la santé, ce qui plaide en faveur d'une informatisation du secteur médical.

Par ailleurs, on parle de davantage de transparence dans les coûts de la santé et de tarifs plus bas pour les médicaments; pour atteindre ces objectifs, l'utilisation des nouvelles technologies de l'information est indispensable. La population elle-même utilise de plus en plus Internet pour s'informer sur les sujets de la santé et, par conséquent, il devient nécessaire d'offrir les meilleurs renseignements car tous les sites consultés ne sont pas fiables.

1. Le secret médical

Toute entité de soins est soumise au secret médical. Le secret médical pourrait en fait s'appeler le secret du patient car lui seul est maître de ses informations. Seul son autorisation donne droit au personnel médical de transmettre ses données. Cependant, le consentement est implicite pour l'échange entre des personnes du corps médical pour autant que les informations concernent le traitement. Voici quelques articles du code pénal suisse qui concernent ce sujet :

1.1. Violation du secret de fonction

Art. 320 CPS[6]

« 1. Celui qui aura révélé un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il avait eu connaissance à raison de sa charge ou de son emploi, sera puni de l'emprisonnement ou de l'amende.

La révélation demeure punissable alors même que la charge ou l'emploi a pris fin.

2. La révélation ne sera pas punissable si elle a été faite avec le consentement écrit de l'autorité supérieure. »

Source : http://www.admin.ch/ch/f/rs/311_0/a320.html

1.2. Violation du secret professionnel

Art. 321 CPS[6]

« 1. Les ecclésiastiques, avocats, défenseurs en justice, notaires, contrôleurs astreints au secret professionnel en vertu du code des obligations, médecins, dentistes, pharmaciens, sages-femmes, ainsi que leurs auxiliaires, qui auront révélé un secret à eux confié en vertu de leur profession ou dont ils avaient eu connaissance dans l'exercice de celle-ci, seront, sur plainte, punis de l'emprisonnement ou de l'amende. Seront punis de la même peine les étudiants qui auront révélé un secret dont ils avaient eu connaissance à l'occasion de leurs

6 Code Pénal Suisse

études. La révélation demeure punissable alors même que le détenteur du secret n'exerce plus sa profession ou qu'il a achevé ses études.

2. La révélation ne sera pas punissable si elle a été faite avec le consentement de l'intéressé ou si, sur la proposition du détenteur du secret, l'autorité supérieure ou l'autorité de surveillance l'a autorisée par écrit.

3. Demeurent réservées les dispositions de la législation fédérale et cantonale statuant une obligation de renseigner une autorité ou de témoigner en justice. »

Source : http://www.admin.ch/ch/f/rs/311_0/a321.html

1.3. Le devoir de discrétion

*« De façon générale la relation soignant patient peut être vue comme un contrat de mandat au sens du code des obligations (**art. 394 ss CO**[7])*

*Ceci impose aux soignants un devoir de fidélité (**art.398 al. 2 CO**[7]) dont découle un devoir de discrétion. »*

Source : http://www.unil.ch/webdav/site/fbm/shared/psyleg/secret_medical_et_ethique_9p.pdf (p.1)

1.4. Serment d'Hippocrate

Hippocrate, médecin de la Grèce antique, est l'un des plus grands personnages de l'histoire de la médecine. Le serment d'Hippocrate est considéré comme l'un des premiers écrits sur la protection des données. Le secret médical a été constitué au fil du temps à partir du texte suivant :

« Je jure par Apollon médecin, par Esculape, Hygie et Panacée, par tous les dieux et toutes les déesses, et je les prends à témoin que, dans la mesure de mes forces et de mes connaissances, je respecterai le serment et l'engagement écrit suivant :

…

7 Code des Obligations

Tout ce que je verrai ou entendrai autour de moi, dans l'exercice de mon art ou hors de mon ministère, et qui ne devra pas être divulgué, je le tairai et le considérerai comme un secret.

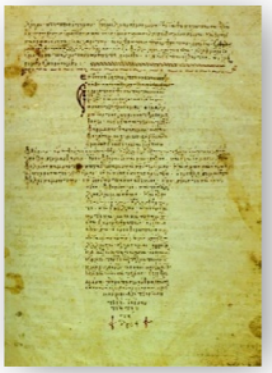
Si je respecte mon serment sans jamais l'enfreindre, puissé-je jouir de la vie et de ma profession, et être honoré à jamais parmi les hommes. Mais si je viole et deviens parjure, qu'un sort contraire m'arrive ! » (Hippocrate, IV^{e} siècle av. J.-C.)

Source : http://www.unil.ch/webdav/site/fbm/shared/psyleg/secret_medical_et_ethique_9p.pdf

Figure 1
Hippocrate

Source : http://www.timone.univ-mrs.fr/medecine/images/hippocrate.jpg

Figure 2
Le serment d'Hippocrate



Source : http://fr.wikipedia.org/wiki/Image:HippocraticOath.jpg

1.5. Ce que dit la loi suisse

La LAMal, (**L**oi sur l'**A**ssurance-**Ma**ladie) stipule que dès le 1er janvier 2006, les prestations des cabinets médicaux doivent être facturées par voie électronique selon le tarif TARMED (**TAR**if **MED**ical). TARMED est le nouveau système tarifaire des prestations médicales ambulantes dans les hôpitaux et dans les cabinets médicaux.

Avec la réorganisation tarifaire TARMED, les assurances veulent voir figurer le plus possible d'informations médicales mais les hôpitaux sont réticents, voulant préserver la sphère privée du patient et la protection des données.

1.6. Les assurances maladies

En Suisse, on différencie l'assurance de base (LAMal) et l'assurance complémentaire ainsi que toutes autres assurances privées. Le médecin, avec l'accord du patient[8] peut fournir à l'assurance de base toutes les informations dont elle a besoin pour effectuer le remboursement de la prestation. Il en est de même pour le remboursement des soins avec l'assurance complémentaire. (Voir Annexe 1 - p.102 pour la facture).

La facture du médecin doit être complète, ce qui veut dire que l'assureur doit pouvoir établir son calcul par rapport aux données écrites. Les diagnostiques figurent sur la facture mais sous forme de codes. Un code "U" peut être demandé par le patient, et seul le médecin-conseil de l'assurance sera autorisé à l'interpréter; ou bien le patient peut exiger que la facture soit directement envoyée à ce médecin-conseil mais n'importe qui ayant accès à cette liste de codes est capable d'en comprendre le sens. (Voir Annexe 2 - p.103).

Le patient doit donner son accord de façon explicite et écrite pour donner les informations à l'assurance privée. La LAMal dit que l'assurance ne peut pas refuser un patient.

8 Accord implicite

2. Qu'existe-t-il en Suisse ?

De nombreux projets ont vu le jour mais peu ont abouti. Les idées et les ambitions ne manquent pas mais le coût et la sécurité posent quand même problème car la santé est un domaine où l'on ne peut pas se permettre d'avoir des fuites… l'enjeu est trop grand.

Chacun souhaite avoir une santé suisse qui ne forme qu'un seul réseau, que nos 26 cantons n'en fassent plus qu'un dans le domaine médical. Pour que cela devienne possible, il faut mettre en place des stratégies, des protocoles communs et une sécurité irréprochable.

A l'heure actuelle, nous avons des dispositifs qui permettent l'échange de données médicales; il s'agit d'entités ici et là qui sont certes très compétentes mais ne travaillent pas ensemble. Les HUG utilisent des applications entre leurs différents départements et unités de soins. Le SIM (**S**ervice d'**I**nformatique **M**édicale) qui fait partie du département d'imagerie et des sciences de l'information médicale, travaille sur la recherche de l'informatique médicale et crée des logiciels. Des DBA[9] (**D**ata **B**ase **A**dministrator) gèrent l'administration des droits d'accès aux données.

La section de médecine dentaire de l'Université de Genève a son propre logiciel géré par des administrateurs qui attribuent des droits différents à des catégories de personnes : par exemple, un étudiant ne pourra pas accéder aux mêmes informations qu'un chef dentiste ou que la comptable. Cependant, le programme n'est pas relié à Internet et ne sera pas intégré au projet de mise en commun, du moins pas pour le moment, ce qui enlève le « poids » de la sécurité des données bien qu'en interne elle puisse tout autant poser problème.

9 Administrateur de base de données

2.1. Les TrustCenters

Les TrustCenters (centres fiduciaires ou centres de confiance) sont des points de recueil pour les données des facturations médicales. Ce sont des organisations propres au corps médical. Il en existe pour le moment 11 dans toute la Suisse qui se partagent plusieurs cantons. Les données sont fournies par les entités médicales et utilisées surtout à des fins statistiques. Un des buts est de surveiller le respect de la neutralité des coûts. Les assurances peuvent obtenir une copie électronique des données de facturation des médecins qui y sont affiliés. Fin 2007, plus de 9'000 médecins étaient rattachés à un TrustCenter.

Source : http://www.newindex.ch/f/produkte_trustcenter.asp

Le TrustCenter :

- S'engage à rendre anonymes les données de facturation qui lui parviennent, en ce qui concerne l'identité de la personne qui établit la facture. Si les informations sur le patient n'ont pas encore été rendues anonymes lors de la réception des données, le TrustCenter doit y remédier immédiatement.
- Doit garantir l'identification et l'authentification des utilisateurs selon les normes de sécurité de la technologie HIN – ASAS ou d'une technologie de sécurité égale (voir 2.3 - p.24). L'accès à ces données sera strictement accordé par des clefs et codes personnels sécurisés.
- Doit permettre l'échange électronique de la facturation selon les dispositions convenues entre les parties contractantes. Il devra cependant veiller à ce que les conditions techniques requises soient données.
- S'engage à respecter la **L**oi sur la **P**rotection des **D**onnées (LPD) et de ce fait prendre des mesures de sécurité techniques et organisationnelles. Il doit évidemment garantir la sécurité des données pendant la transaction sur Internet.

2.1.1. Clientèle des TrustCenters

Tableau 1

Données de clientèle[10] TC (TrustCenter)

TrustCenter	Cantons	Nombre
Ctésias	FR, **GE**, JU, NE, VS	**1'914**
GallOnet	AI, AR, GL, GR, SG, TG	769
hawatrust	ZH	629
medkey	LU, NW, OW, SZ, UR, ZG	556
PonteNova	BE, SO	1'480
syndata	BL, BS, SO	715
TC Aargau	AG, SO	618
TC Thurcare	AI, AR, GL, SG, SH, TG	349
TC ticino	TI	305
trustmed	ZH	815
ZüriDoc	ZH	507
Total		**8'657**

Vue d'ensemble au 30.09.06

Source : http://www.newindex.ch/f/aktuelles_kundenstand.asp

2.1.1.1. Ctésias

Ctésias est le TrustCenter des cantons romands. Cette entreprise est spécialisée dans la collecte et l'analyse de données. Plus de 3 millions de factures sont analysées chaque année. Elles peuvent être transmises aux assurances au format XML[11].

10 Médecins privés, cabinets médicaux, hôpitaux…

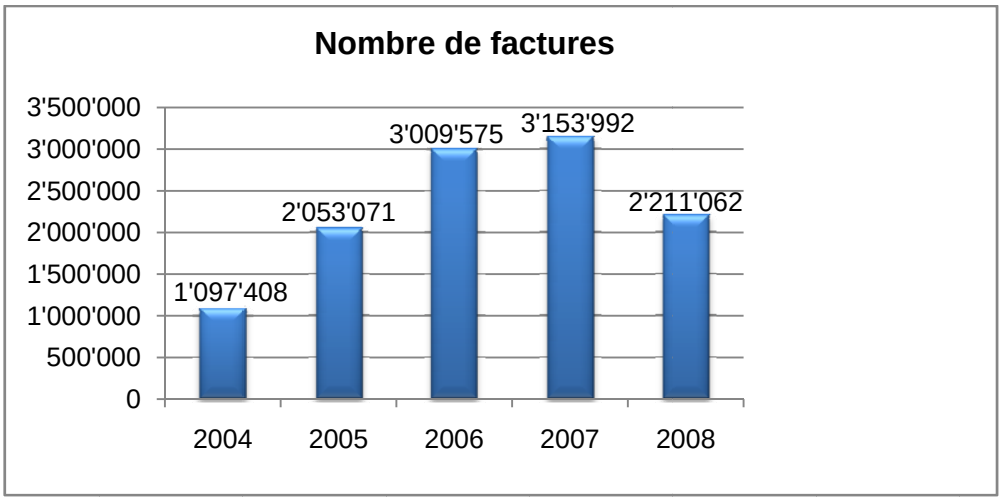
11 Langage informatique de description de documents en le structurant de façon standard

Tableau 2

Statistiques du nombre de factures dans le miroir[12] du cabinet

Année	Nombre de factures
Total 2004	1'097'408
Total 2005	2'053'071
Total 2006	3'009'575
Total 2007	3'153'992
Total 2008	**2'211'062**

En compte au 12.09.2008



Source : http://www.ctesias.ch/index.php?option=com_content&task=view&id=12&Itemid=27

2.1.2. TrustX

TrustX est une interface entre l'entité médicale et le TrustCenter qui permet d'exporter et de transmettre les facturations des patients. Tous les TrustCenters utilisent le logiciel TrustX. Les données sont entièrement cryptées et le destinataire est identifié. Les informations sont toujours anonymes, ni le personnel médical, ni le patient ne figurent durant le processus. TrustX-Cabinet peut être intégré au logiciel médical que le cabinet dispose déjà ou veut acquérir.

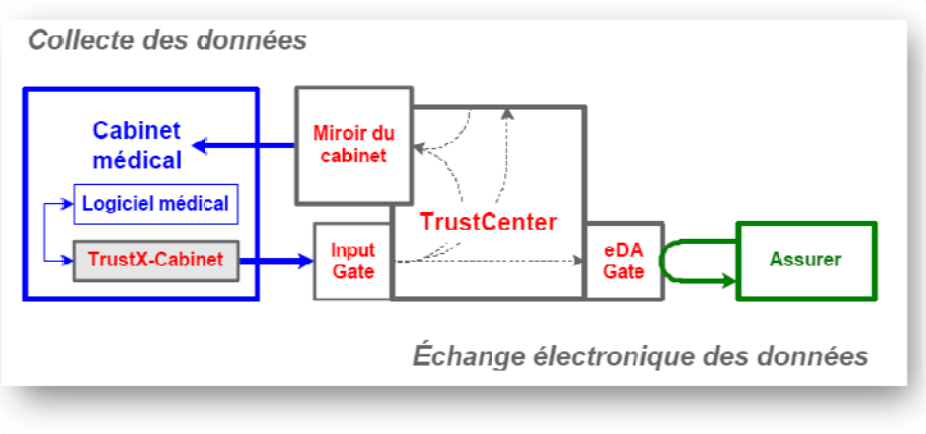
Le miroir de l'utilisateur du logiciel permet de faire des statistiques standardisées de ses propres données en ligne mais aussi entre collègues.

12 Outil pour faire des statistiques en ligne sur les données du cabinet

Avec l'accord du patient, l'assureur peut se procurer une copie électronique de la facture auprès du TrustCenter.

Le cabinet médical transmet les données à son TrustCenter qui vérifie l'identité de l'émetteur; elles sont alors mises à la disposition de l'assureur.

Figure 3
Ensemble du processus de l'échange des données

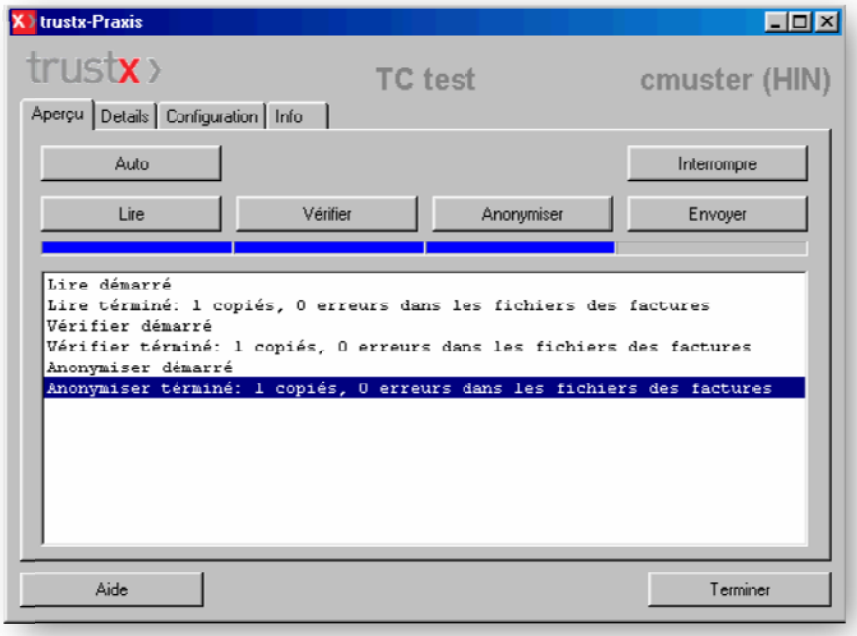


Source : http://www.trustx.ch/trustx-praxis/documents/Interface_TrustX-Cabinet_pour_editeurs_logiciels.pdf (p.5)

Toutes les données doivent être transmises au TrustCenter pour qu'il puisse effectuer les statistiques.

Le miroir du cabinet permet de faire des comparaisons avec d'autres cabinets qui travaillent dans le même domaine. Le logiciel médical est celui qu'utilise le médecin. TrustX-Cabinet qui peut-être installé dans le cabinet, rend les données des patients anonymes et les transmet à « l'Input Gate » où des programmes réceptionnent, contrôlent l'anonymat et font la transmission des données des décomptes. L' « eDAGate » met à disposition des assurances les factures électroniques.

Figure 4
Anonymisation d'une facture



Source : http://www.trustx.ch/trustx-praxis/documents/Interface_TrustX-Cabinet_pour_editeurs_logiciels.pdf (p.20)

2.1.2.1. Trois façons de transférer les données :

- Directement depuis le système d'administration du cabinet médical avec le module du logiciel TrustX-Cabinet (voir Figure 4).
- Avec TrustX-Cabinet en transmettant les factures dans une liste fournie par le logiciel via une interface utilisateur.
- Avec un centre de clearing[13]; les données peuvent être directement transmises au TrustCenter.

2.1.2.2. Processus de facturation

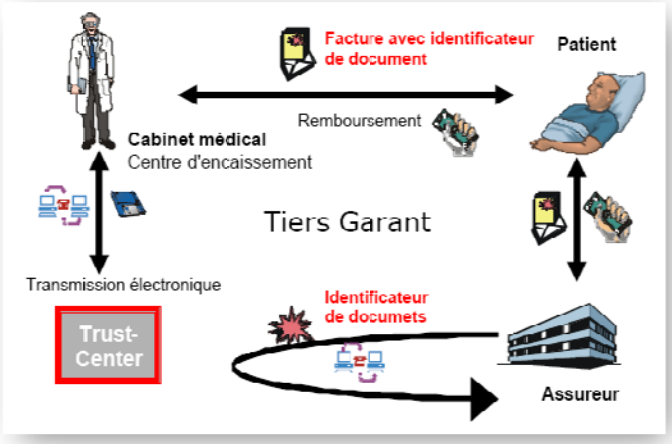
Il y a 2 façons de payer les factures. Le principe d'« aller-chercher », qui passe par un Tiers Garant et le principe « apporter », qui utilise un Tiers Payant.

Pour le Tiers Garant, un Token (identificateur unique) est imprimé sur le justificatif du remboursement. Le médecin envoie la facture directement au patient qui la transmet à

13 L'utilisation de décomptes électroniques permet de répondre à l'obligation de transfert électronique de données.

l'assurance pour se faire rembourser. Cette dernière peut obtenir une copie de la facture dans le TrustCenter grâce à ce Token.

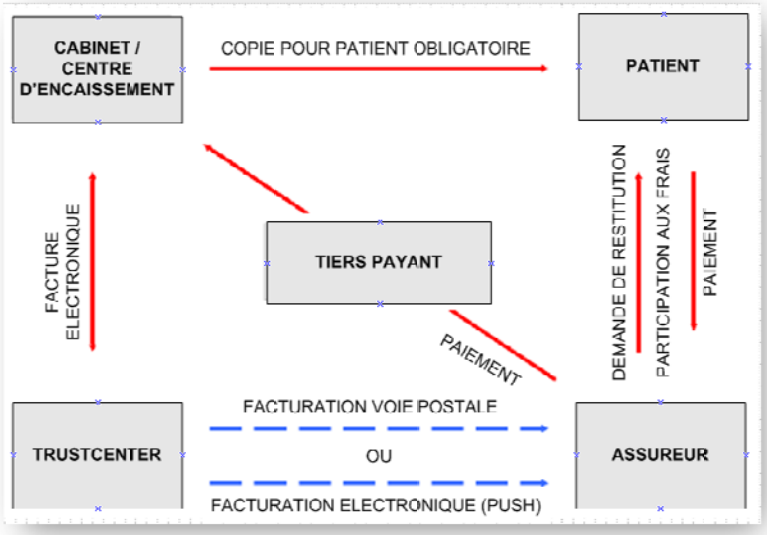
Figure 5
Facturation « aller-chercher » (Tiers Garant)



Source : http://www.trustx.ch/trustx-praxis/documents/Interface_TrustX-Cabinet_pour_editeurs_logiciels.pdf (p.8)

Pour le principe de Tiers Payant, le TrustCenter joue l'intermédiaire entre l'assurance et le médecin.

Figure 6
Facturation « apporter » (Tiers Payant)



Source : http://www.trustx.ch/trustx-praxis/documents/Interface_TrustX-Cabinet_pour_editeurs_logiciels.pdf (p.6)

2.1.2.3. Que faut-il pour utiliser TrustX ?

Il faut un client ASAS-HIN (voir 2.3 - p.24) qui garantit l'authentification de l'émetteur des données ainsi que le cryptage end-to-end (S/MIME)[14] (voir 4.5 - p.77), l'identité des patients et les images électroniques des factures.

- Un abonnement à HIN (voir 2.3 - p.24)
- Un des systèmes d'exploitation suivants :
  - Windows : « Windows 2000 », « Win XP », « Windows Vista »
  - Mac : à partir de « OS X 10.3 »
- Une connexion Internet ADSL[15]

Source : http://www.trustx.ch/f/system_datenanlieferung_1.asp

2.2. NewIndex

NewIndex a créé le concept des TrustCenters. Son objectif est de contribuer d'une part à l'amélioration de la transparence du système de santé par des projets concrets et, d'autre part, à l'exploitation des données médicales afin d'optimiser la qualité et la rentabilité du système de santé suisse. NewIndex est par ailleurs un centre de compétences et de prestations dans le domaine des statistiques et de l'analyse des données de la communauté médicale de notre pays. L'entreprise a saisi l'opportunité d'instaurer la parité des données grâce aux TrustCenters.

2.3. HIN

Health **I**nfo **N**et est une plateforme extranet sécurisée du domaine de la santé en Suisse. Il joue le rôle d'autorité de certification pour la distribution de clefs publiques (voir 4.4.7 - p.74). Le HIN est un centre de calculs et de technologie de sécurité. Il propose aux professionnels de la santé suisse une communication par e-mail sécurisée et conforme à la protection des données. Les abonnés sont donc en mesures d'envoyer des données sensibles telles que le dossier d'un patient, des

14 Protocole de sécurité d'envoi d'e-mail

15 Connexion « haut débit »

résultats d'analyses, un compte-rendu de sortie d'hôpital etc., tout ceci en toute sécurité.

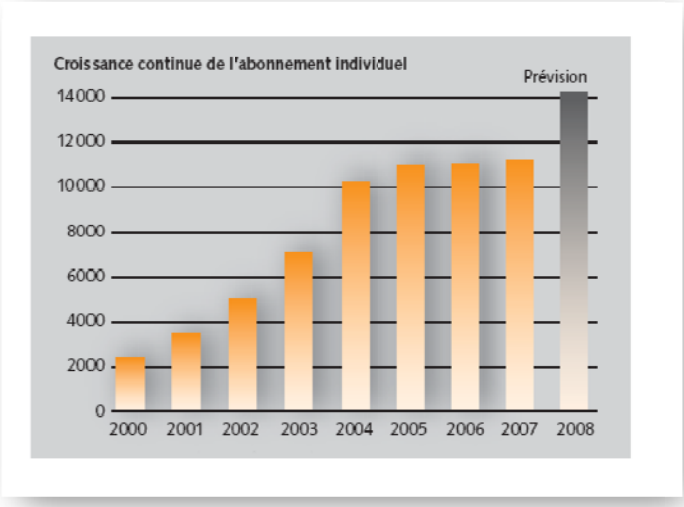
HIN ne propose pas seulement l'envoi de mails sécurisés mais aussi celui de données de facturation aux TrustCenters ou aux assurances ainsi qu'un accès authentifié aux dossiers des patients dans les lieux médicaux. HIN permet aussi de procéder à la commande de médicaments pour un patient : 80% des pharmacies peuvent communiquer via un réseau nommé OVAN.

OVAN (**O**fac **V**alue **A**dded **N**etwork) est un réseau virtuel sécurisé appelé VPN (**V**irtual **P**rivate **N**etwork) destiné au secteur médical.

Fin 2007, il y avait plus de 11'000 clients individuels et 120 institutions connectés à la plateforme HIN.

HIN n'est pas la seule plateforme qui existe en Suisse mais, à ce jour, elle est la plus utilisée. Cela ne veut pas dire que dans un futur proche cela sera encore le cas. MediPort ou H-Net (voir 2.4 - p.30) proposent aussi des services similaires.

Figure 7
Croissance continue de l'abonnement individuel



Source : http://www.hin.ch/f/pdf/gb_2007.pdf

Les différents secteurs qui sont abonnés à HIN :

- Médecins
- Hôpitaux et cliniques

- Services de soins à domicile
- Laboratoires
- Caisses maladie
- TrustCenters
- Centres de facturation
- Pharmacies via le réseau OVAN
- Pharmacies de vente par correspondance
- Organisations professionnelles
- Sociétés cantonales de médecins et sociétés spécialisées

Le service de radiologie des HUG, de l'hôpital cantonal de Lucerne ainsi que la clinique de StephansDorm à Saint-Gall utilisent maintenant aussi HIN pour partager les radios des patients.

2.3.1. ASAS

ASAS (**A**rpage **S**ecurity and **A**ccess **S**ervices) est un système de sécurité adopté par la plateforme HIN. Il utilise des normes de sécurité connues.

ASAS :

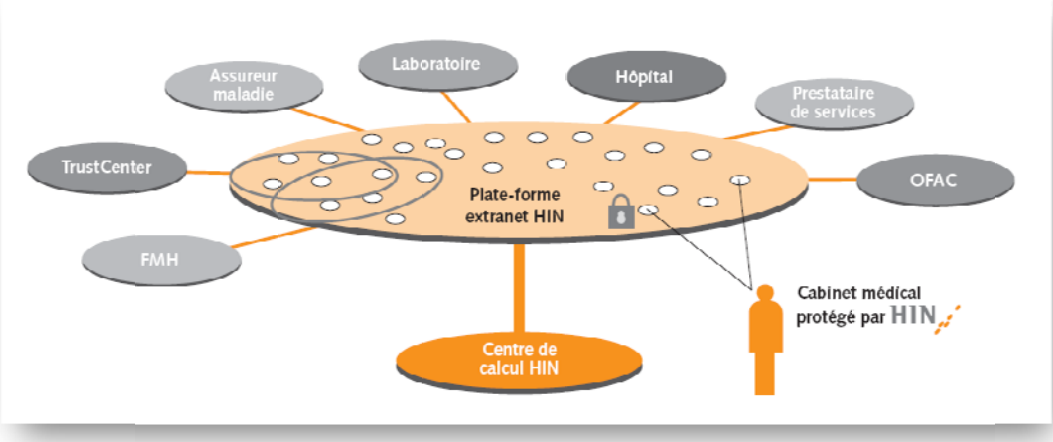
- Génère des clefs publiques et privées selon l'algorithme RSA (voir 4.4.7.2 - p.75)
- Gère les clefs publiques et les certificats selon la norme X.509[16] (voir 4.7.1 - p.74)
- Propose un tunnel SSL à 168 bits (voir 4.4.6.2 - p.74)
- Autorise un cryptage "end-to-end" à 1'024 bits et le (S/MIME) (voir 4.5 – p.77)
- Accepte les signatures digitales (S/MIME)
- Authentifie les personnes en ligne OCV (**O**nline **C**ertificate **V**alidation)
- Supporte le **S**ingle-**S**ign-**O**n (SSO) (voir 4.6 - p.77)

Son infrastructure utilise les clefs publiques PKI (voir 4.4.7.1 - p.74) qui sont gérées sur le serveur ASAS. Seul l'utilisateur connait sa clef privée (voir schéma p.76).

16 Norme sur les certificats d'authentification

Le système (client) ASAS est installé sur le poste de l'utilisateur et le serveur HIN ASAS se trouve dans le centre de calcul HIN.

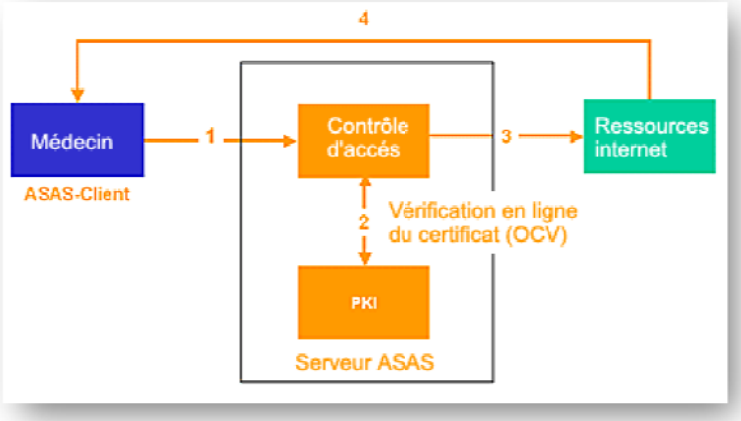
Figure 8
Plateforme HIN et clients



Source : http://service.escapenet.ch/publisher/pictures/280/181083/Factsheet_HIN_Abo_f.pdf

Avec l'**A**ccess **C**ontrol **S**ervice (ACS) de HIN, les hôpitaux mettent à disposition du personnel médical externe les informations des patients. Une liste de contrôle d'accès est établie par l'hôpital dans le centre de calcul de HIN. HIN est responsable de la sécurité et assure un accès rapide et facile aux données grâce à un processus d'identification, le **S**ingle-**S**ign-**O**n (SSO) (voir 4.6 - p.77).

Figure 9
Schéma de topologie HIN Access Control Services



Source : http://www.hin.ch/f/hinaccess_funktionalitaet.htm

Explication du schéma précédent :

1. Le médecin veut obtenir des informations d'un patient à travers le réseau, il passe par le contrôle d'accès ACS.
2. L'ACS vérifie le certificat en ligne (OCV) en regardant dans le serveur ASAS la clef publique PKI (voir 4.4.7.1 – p.74).
3. Si tout est correct, l'ACS accède aux ressources Internet.
4. Les informations demandées par le médecin lui parviennent directement.

Il est possible de conclure deux abonnements par client. Le premier sera uniquement utilisé par le médecin et le deuxième par l'équipe du cabinet médical, et par l'administration pour l'envoi des factures aux TrustCenters, pour la commande de médicaments etc. Ce deuxième abonnement ne permet pas de correspondre avec d'autres cabinets pour l'obtention d'informations sur des patients. Ainsi la sphère privée du patient est garantie entre lui et son médecin.

2.3.2. HIN MailGateway

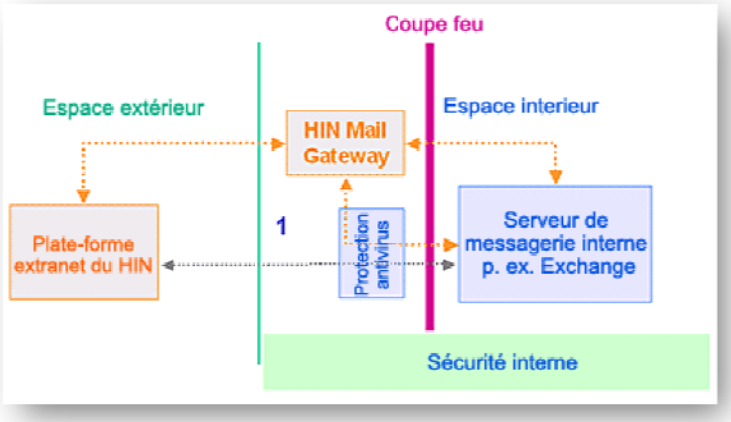
HIN MailGateway est une passerelle pour l'envoi d'e-mail; elle est proposée aux clients tels que les hôpitaux et les laboratoires. Ce service offre :

- Une paire de clefs avec l'algorithme RSA (voir 4.4.7.2 - p.75) pour crypter et décrypter les mails et les pièces jointes.
- Une signature numérique (voir 4.7 - p.78) qui permet l'**authenticité** et l'**intégrité** des données.
- Un certificat électronique avec la norme X.509 (voir 4.7.1 - p.78).
- Le protocole S/MIME (voir 4.5 - p.77).

HIN MailGateway se trouve dans la zone démilitarisée (DMZ)[17]. La connexion en dehors de la plateforme extranet est protégée par ASAS (voir 2.3.1 - p.26) et SSL (voir 4.4.6.2 - p.74).

17 Sous-réseau isolé par un Firewall entre le réseau interne et externe

Figure 10
Schéma de topologie HIN MailGateway



Source : http://www.hin.ch/f/hinmail_funktionalitaet.htm

Afin de se protéger, HIN avertit ses clients que, bien qu'il ait mis en place un dispositif très sûr, Internet ne l'est pas pour autant et qu'il est donc conseillé de prendre des mesures adéquates telles qu'un anti-virus.

*« **Sécurité et protection des données***

*Le client déclare savoir que les données sont transportées sur l'Internet par un réseau de télécommunications public. Bien que les paquets de données soient codés, **les identifications d'expéditeur et de destinataire ne le sont pas et peuvent donc être lues par des tiers, comme dans le courrier normal.** Sécurité HIN apporte une attention particulière à la sécurité de ses services. Le système de sécurité ASAS est notamment fondé sur un procédé de cryptage très évolué. **Le chiffrement interdit en principe à toute personne non autorisée de lire les données confidentielles du client.** Mais malgré toutes les précautions de sécurité, même à l'avant-garde des techniques, **la sécurité ne peut être garantie avec une parfaite certitude, ni chez HIN, ni chez le client.***

Risques de l'Internet

Le client déclare donc avoir connaissance des risques suivants, liés à l'utilisation de l'Internet : la connaissance insuffisante des systèmes et le manque de précautions de sécurité peuvent faciliter les accès non autorisés; il incombe donc

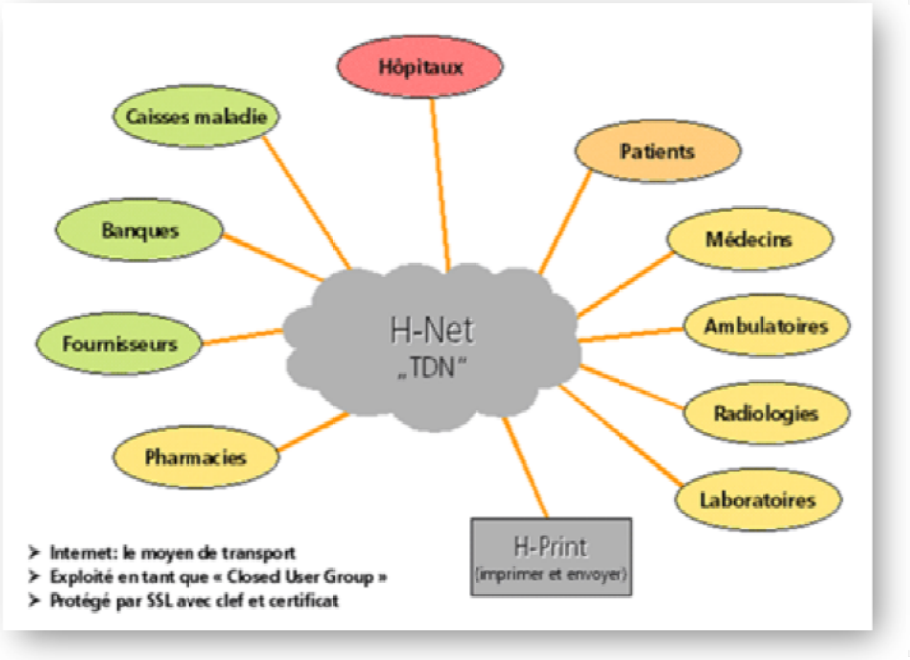
au client de s'informer des précautions de sécurité nécessaires; ***il existe un risque latent qu'un tiers profite du moment ou l'utilisateur est raccordé à l'Internet pour accéder secrètement à l'ordinateur du client;*** *HIN recommande la mise en place d'une protection interne par pare-feu (firewall), à moins que le raccordement ne soit réalisé directement par HIN en tant que fournisseur d'accès à Internet; en outre, il existe toujours le risque que des virus provenant de l'Internet infectent l'ordinateur du client; HIN recommande l'emploi de logiciels antivirus, qui peuvent protéger le client contre ces risques. »*

Source : http://www.hin.ch/f/pdf/rahmenbedingungen_f.pdf

2.4. H-Net

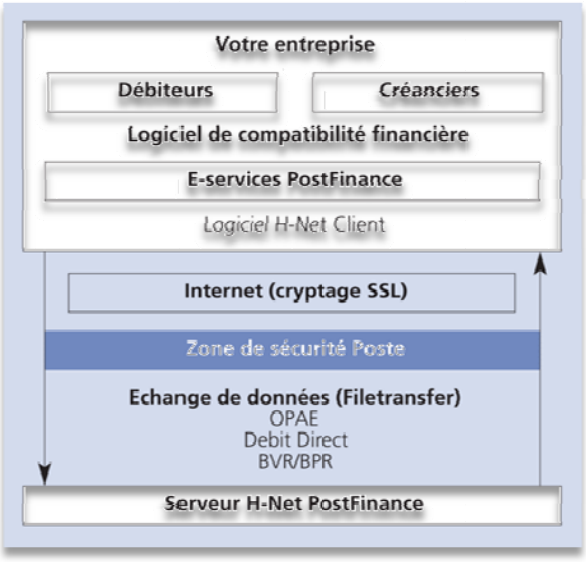
H-Net est une plateforme de transaction entre certains hôpitaux, cabinets médicaux et autres organes de santé. Elle travaille directement avec la poste suisse et son service PostFinance pour le transfert de factures.

Figure 11
Réseau H-Net



Source : http://www.avintis.com/index.php?option=com_content&view=category&layout=blog&id=13&Itemid=15

Figure 12
Fonctionnement du service PostFinance



Source : http://www.postfinance.ch/pf/content/fr/seg/biz/product/eserv/filetransfer/hnet.html

2.5. Système Covercard®

Ofac[18] et santésuisse ont développé un système appelé Covercard® qui permet aux professionnels de la santé d'avoir un suivi en ligne sur les informations administratives des assurés lors de la prise en charge du patient.

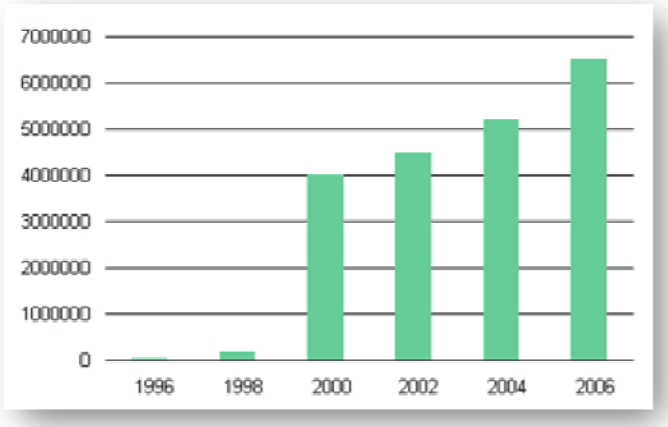
Figure 13
Carte Covercard®

Source : http://www.hin.ch/f/pdf/HIN_Covercard_Service_factsheet.pdf (p.4)

58 assurances utilisent ce système, ce qui représente 6.5 millions d'assurés en 2006. Avec plus de 2'500 prestataires qui utilisent Covercard® chaque jour, c'est plus de 60'000 requêtes qui sont envoyées quotidiennement au serveur.

18 Coopérative professionnelle des pharmaciens suisses

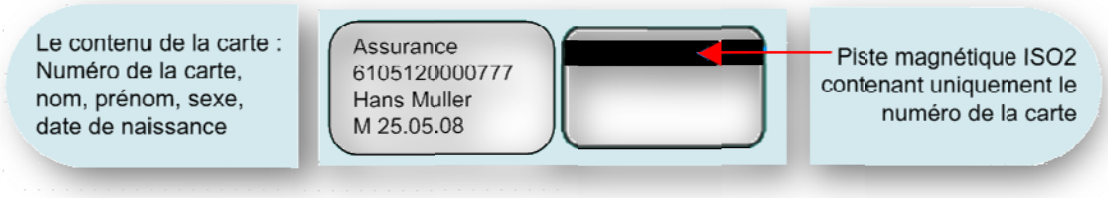
Figure 14
Nombre de porteurs de carte Covercard®



Source : http://www.covercard.net/FRN/

Les assurances envoient les données des assurés au serveur Covercard®. Chaque assuré possède une clef univoque inscrite sur la carte et encodée sur la bande magnétique.

Figure 15
Données et codes Covercard®



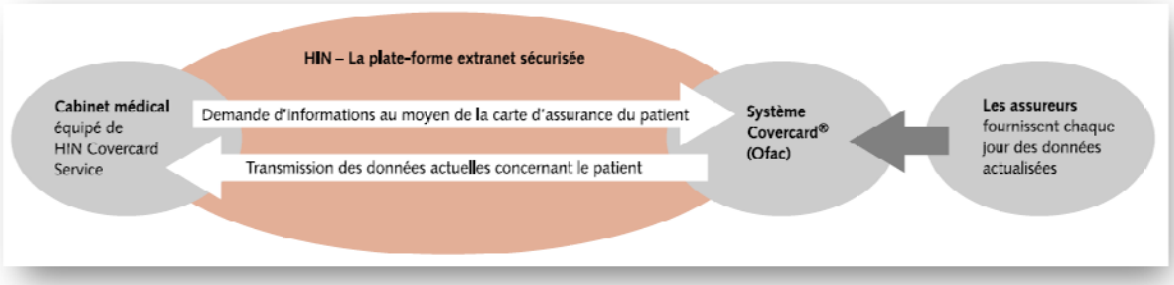
Source : http://www.covercard.net/FRN/

Il y a plusieurs façons d'accéder aux données :

- En saisissant le numéro de la carte sur un clavier téléphonique, une boîte vocale demande le mot de passe qui aura été donné auparavant au personnel médical. Cette solution est pratique pour les consultations à domicile.
- Par un lecteur de carte bancaire, la sécurité étant basée sur les normes bancaires.
- Par le site Internet de www.covercard.ch qui interroge directement le serveur en utilisant le protocole SSL3 (voir 4.4.6.2 - p.74) et la norme X.509 (voir 4.7.1 - p.78).

- Par le réseau OVAN, réseau virtuel (VPN) qui a l'avantage d'avoir une bande passante à haut débit permettant un accès rapide aux données.
- En passant par les plateformes sécurisées HIN ou H-Net qui sont affiliées au système Covercard®.

Figure 16
Processus d'échanges de données avec la Covercard®

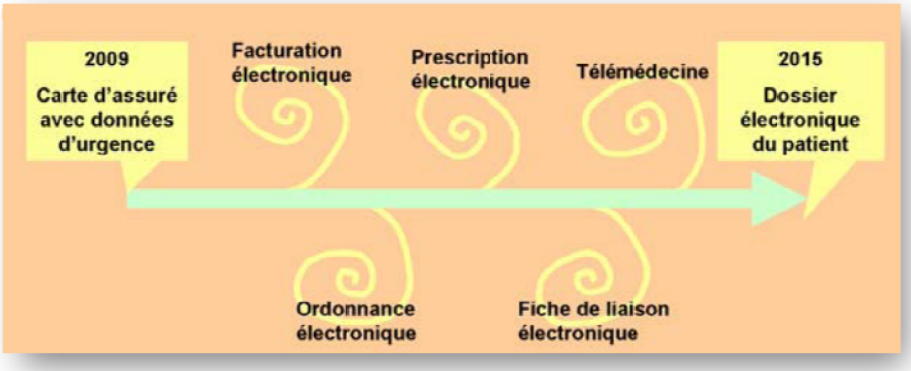


Source : http://www.hin.ch/f/pdf/HIN_Covercard_Service_factsheet.pdf (p.3)

2.6. Stratégie eHealth

La stratégie eHealth, cybersanté suisse, adoptée par le conseil fédéral en juin 2007 est en application depuis début 2008. Les principaux objectifs de cette stratégie sont d'atteindre d'ici 2015 la mise en place progressive du **dossier électronique du patient** et d'un **portail de santé** qui permettra à chacun d'accéder à son propre dossier médical. Les patients devront pouvoir choisir qui aura accès ou non à ce dossier. Par cybersanté, on entend l'utilisation du **TIC** (**T**echnologie de l'**I**nformation et de la **C**ommunication). La stratégie eHealth attache une grande importance à la sécurité. Il est évident que plus le système de santé électronique que l'on propose est développé, plus la sécurité doit être renforcée. Cette stratégie ne compte pas informatiser ce qui existe à ce jour mais reprendre entièrement depuis le début puis mettre en réseau.

Figure 17
Planning du projet de la stratégie eHealth



Source : stratégie eHealth p.9

« Dans le système de santé suisse, chaque individu peut autoriser les spécialistes de son choix à accéder, à tout moment et en tout lieu, à d'importantes informations pertinentes sur sa personne et bénéficier de prestations. Il participe activement aux décisions concernant son comportement et ses problèmes liés à la santé, renforçant ainsi sa culture sanitaire. ***Les technologies de l'information et de la communication sont utilisées de manière à assurer la mise en réseau des acteurs du système de santé et à créer des processus de meilleure qualité, plus sûrs et plus efficaces.*** *»*

Tiré du document : stratégie eHealth p.3

« Dans le domaine de la santé, le caractère contraignant, la protection des données et la sécurité des données jouent un rôle tellement important que de nombreux processus ne peuvent avoir force exécutoire et être sûrs et efficaces que si les patients et les prestataires sont identifiés de manière fiable (p. ex. avec une carte de santé pour les patients et une carte de professionnel de la santé munie d'une signature numérique pour les fournisseurs de prestations). »

Tiré du document : stratégie eHealth p.9

La priorité de la stratégie eHealth est axée sur la sécurité de l'information et la protection des données.

2.6.1. Publifocus

Le Publifocus, aussi appelé PubliForum ou focus group, est une méthode participative qui a été développée par le centre d'évaluation des technologies suisses TA-SWISS. Elle sert à intégrer des citoyens à des prises de décisions politiques dans le domaine de la technologie.

Un Publifocus a été organisé avec pour thème « eHealth et le dossier électronique du patient ». Quatre groupes ont été formés. Un groupe de francophones, un de germanophones, un d'italophones et un dernier groupe constitué de représentants du domaine de la santé. Un questionnaire leur a été soumis à l'avance avec les thèmes du débat animé par des professionnels.

Le but de ce Publifocus était de connaître les différents points du vue des futurs détenteurs du dossier électronique.

Le principal point que l'on peut retenir de ce Publifocus est que les avantages concernant le dossier électronique du patient sont bien plus présents que les risques liés à la sécurité.

Le fait que l'e-banking utilise ce genre de technologie nous fait constater que cela rassure les participants de ce débat. Les banques arrivent bien à assurer les données, alors pourquoi pas avec les données des patients ? Tout repose sur une bonne gestion des garde-fous mais cela relève des décisions des politiciens.

> *« Le but du hacker est de faire virer l'argent d'un compte en banque sur le sien, je ne vois pas quelle utilité il aurait à pirater mon dossier électronique, ma santé ne l'intéresse pas »* relève un participant du Publifocus. Un autre n'est pas tout à fait du même avis. *« Même des codes que l'on considère comme inviolables, le sont pourtant... »*

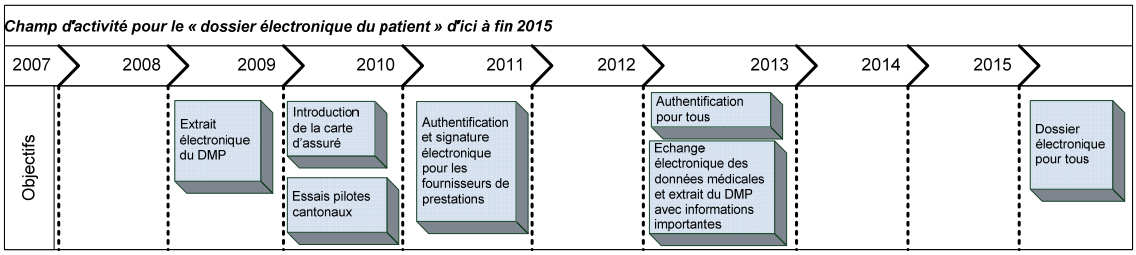
Certaines personnes un peu plus sceptiques relèvent le fait que la sécurité ne peut pas être assurée à cent pour cent, mais autant dans l'informatique que dans d'autres domaines.

2.6.2. Objectifs pour le dossier électronique du patient

Un Planning a évidemment été réalisé avec des objectifs pour chaque phase.

Figure 18

Planning du dossier électronique du patient



Objectif A1 :

« D'ici à fin 2008, les normes d'un extrait électronique du dossier médical personnel, contenant les informations nécessaires au traitement, sont définies. Les conditions pour l'introduction sont décrites. »

Une pré-phase du dossier électronique est envisagée, elle consiste à mettre quelques données sur ce dernier et de voir comment cela se passe avant de demander au personnel médical de le remplir entièrement.

Objectif A2 :

*« **La carte d'assuré est introduite en 2009** (avec les options facultatives pour les données médicales personnelles). »*

Objectif A3 :

*« A partir de 2009, les cantons peuvent réaliser **des essais-pilote en matière de cybersanté sur la base de la carte d'assuré**. »*

Objectif A4 :

*« D'ici à fin 2010, tous les fournisseurs de prestations disposent de **l'authentification sécurisée et de la signature électronique juridiquement valable** – celles-ci sont utilisées pour l'échange électronique de données. »*

La carte professionnelle de santé pourrait faire l'objet d'un moyen sûr et légal d'assurer l'authentification des échanges de données.

Objectif A5 :

« Début 2012, ***l'authentification sécurisée est établie pour toute personne résidant en Suisse*** *– avec une* ***option pour la signature électronique légale.*** *»*

La carte d'assuré pourrait rendre possible l'authentification sécurisée. Une clef d'accès serait donnée à chacun et la signature électronique pourrait être demandée.

Objectif A6 :

« D'ici à fin 2012, l'échange par voie électronique de données médicales entre les partenaires du système de santé est structuré et ***n'entraîne plus ni rupture de médias, ni pertes.*** *Tous les hôpitaux de soins somatiques aigus, tous les réseaux de soins intégrés et au moins 50% des médecins libéraux ont adopté l'extrait électronique du* ***dossier médical personnel qui comporte les informations importantes pour le traitement.*** *»*

Cet objectif ne peut être effectué que si l'objectif A1 a été réalisé.

Objectif A7 :

« D'ici à fin 2015, toutes les personnes en Suisse peuvent, indépendamment du temps et du lieu, ***donner aux prestataires de leur choix l'accès électronique aux informations nécessaires à leur traitement ("dossier électronique du patient").*** *»*

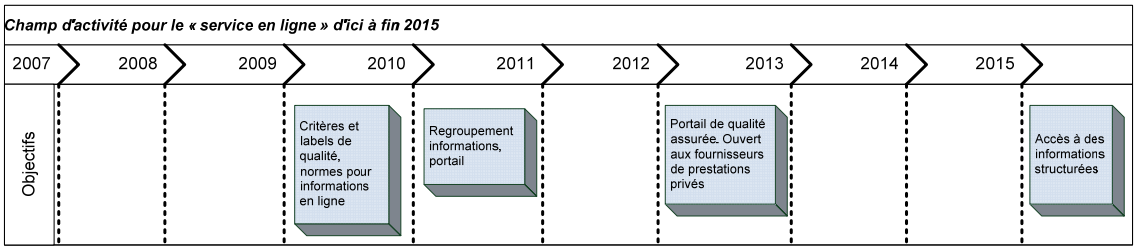
Tiré du document : stratégie eHealth p.4

2.6.3. Objectifs pour le service en ligne

Trop d'informations sur la santé existent sur Internet et la population ne sait plus quelles sont les sources crédibles, c'est pourquoi l'Etat veut mettre en ligne des documentations et des recommandations sur le risque en matière de santé; les gens pourront alors les consulter en toute confiance.

Figure 19

Planning du service en ligne



Objectif B1 :

« D'ici à fin 2009, on examine quelles normes de qualité dans la perspective d'un regroupement des informations en ligne relatives à la santé doivent être introduites. »

Objectif B2 :

« D'ici à fin 2010, ***les informations en ligne*** *proposées par la Confédération, les cantons et les communes en matière de santé ainsi que par les organisations* ***internationales sont accessibles sur un portail de la santé commun.*** *»*

Comme il existe déjà des portails dans certains pays et même dans certains de nos cantons, cet objectif serait de les mettre en commun et d'offrir à la population un lieu de consultation; ils pourraient alors en toute confiance trouver les informations les concernant soit géographiquement soit linguistiquement. L'OMS[19] serait raccordée à ce portail.

Objectif B3 :

« D'ici à fin 2012, les offres d'informations sur le portail de la santé répondent aux critères de qualité. ***Les fournisseurs de prestations privés peuvent se raccorder au portail.*** *»*

19 Organisation Mondiale de la Santé

Objectif B4 :

« D'ici à fin 2015, ***l'accès sécurisé des citoyens à leur dossier électronique de santé sur le portail de la santé*** *leur permet de consulter des informations structurées et spécifiques. »*

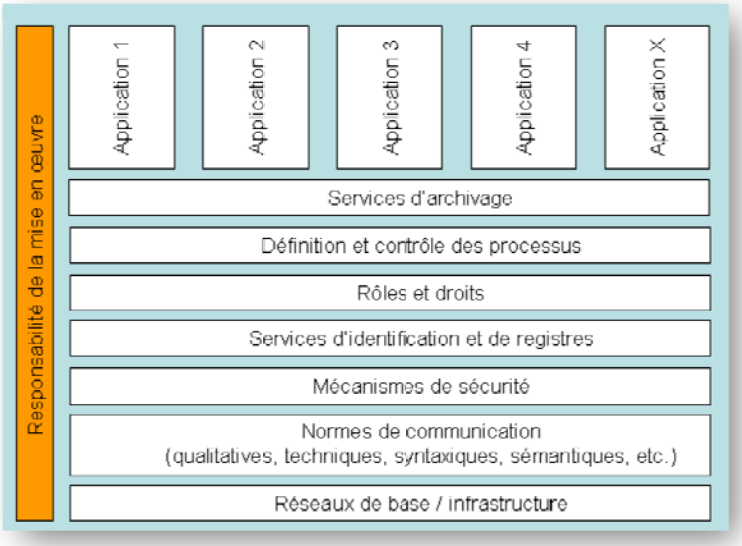
Le dossier électronique du patient serait raccordé au portail de santé et permettrait aux citoyens d'administrer les informations en donnant les droits de lecture et/ou de modification.

Tiré du document : stratégie eHealth p.5
Source : http://www.bag.admin.ch/themen/krankenversicherung/04108/index.html?lang=fr

Un portail en ligne existe déjà au niveau européen, il a été créé en 2006 par l'Union européenne et sert à réunir des informations sûres et exactes permettant à la population de consulter des sites Internet sur la santé publique (voir Objectif B2).

Une autre étape est de définir des normes et des lois concernant la cybersanté et de mettre en place des architectures et interfaces communes avec les autres pays afin d'améliorer l'interopérabilité entre eux.

Figure 20
Conditions-cadres et accords politiques et légaux



Source : stratégie eHealth p.38

2.6.4. Service qualité et label

Health **O**n the **N**et (HON) est une association non gouvernementale de référence pour la mise en ligne d'informations dans le domaine de la santé. Elle a créé sa propre charte, le HONcode qui permet l'obtention d'un certificat sur la qualité des données médicales en ligne; elle est très utilisée en Suisse de même que d'autres entreprises d'accréditation, telles que :

- TRUSTe : Compagnie sponsorisée notamment par Microsoft et AOL qui certifie la confidentialité des informations sur Internet.
- MedCircle / MedCertain : Organisation qui aide à apprendre à reconnaître les bonnes informations à mettre sur un site web.
- Web Medica Acreditada (WMA) : Service d'accréditation pour les sites Internet espagnols ou d'Amérique latine.
- URAC : Organisation américaine qui encourage la qualité dans le domaine de la santé et promeut les programmes de certifications et d'accréditations.
- eCH : Créé et adopte des normes de Cyberadministration. Vérifie la qualité des informations médicales et sanitaires sur Internet.

L'OMS réfléchit à la mise en place d'un nom de domaine « **.**health » ce qui améliorerait le niveau et la qualité des informations médicales sur Internet.

Figure 21
Sceau HONcode, preuve de certification

Source : www.hon.ch/HONcode/

Les demandes de certification peuvent être rejetées. HON exige que le contenu du site soit en accord avec la législation du pays pour lequel il est destiné. La fondation assure la confidentialité des données transmises. Il y a plusieurs principes à respecter :

L'autorité

- Il est obligatoire de mettre le nom de la personne qui a donné l'information et de mentionner son statut (médecin, infirmier….)

La confidentialité

- Même si le site Internet ne met pas de données sensibles en ligne, la confidentialité doit être respectée. Il faut explicitement informer sur l'utilisation des informations récoltées, par exemple si une base de données recense les adresses e-mails ou les informations échangées et qui a accès à celles-ci. Une section bien visible doit être consacrée au code de confidentialité adopté.

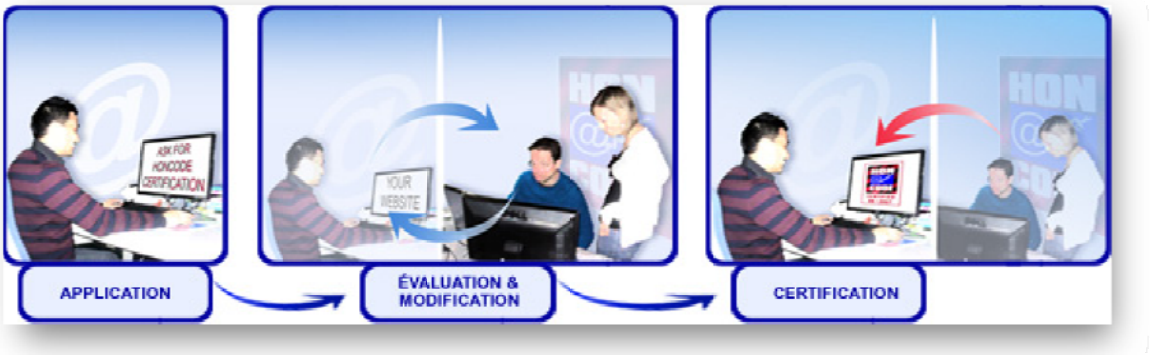
Origine et datation des informations

- Le domaine médical évolue très vite et les informations peuvent devenir obsolètes et même inexactes en très peu de temps; il faut donc mettre la date de publication et de mise à jour de l'information.

La preuve

- Toute information doit pouvoir être prouvée.

Figure 22
Processus de certification



Source : http://www.hon.ch/HONcode/Webmasters/StepByStep/StepByStep_f.html

Application

Prendre connaissance des principes de HONcode, remplir le formulaire de demande de certification.

Evaluation et modification

Les principes énoncés ci-dessus sont analysés par un spécialiste de HONcode.

Certification

Afficher le sceau sur la page d'accueil de son site Internet.

Figure 23

Processus de réévaluation

Source : http://www.hon.ch/HONcode/Webmasters/StepByStep/StepByStep_f.html

Validité du certificat

La validité du certificat est d'une année. Tout au long de celle-ci, le site est supervisé.

Processus de réévaluation

Le site est réévalué tout au long de l'année comme au moment de la demande de certification.

Extension du certificat

Vérification que les changements demandés ont bien été faits, ainsi la prolongation du certificat pourra s'effectuer.

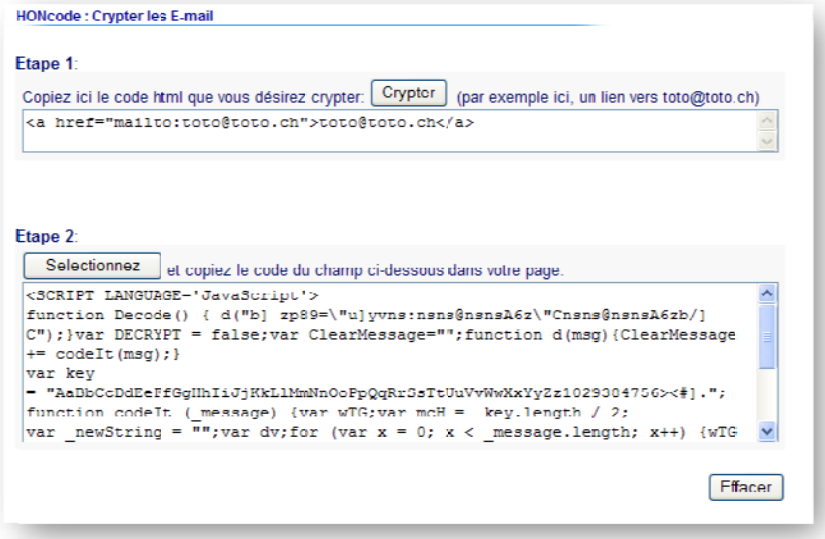
Figure 24

Barre d'outils de certification HONcode

Source : http://www.hon.ch/HONcode/Plugin/Plugins_f.html

Le site HONcode permet de crypter les adresses e-mail. Il suffit de suivre la démarche de la Figure 25. Après avoir tapé son adresse et cliqué sur le bouton « Crypter », le code se génère, il faut ensuite le copier dans son site web.

Figure 25
Générateur de cryptage d'adresses e-mail



Source : https://www.hon.ch/HONcode/email_encrypt_f.html

2.6.5. Le dossier électronique du patient

A l'heure actuelle, les données médicales des patients sont stockées un peu partout, sur des ordinateurs personnels, en réseau dans des établissements de soins ou encore dans des dossiers papier. A chaque fois que vous allez chez un médecin vous devez refaire les analyses qu'un autre médecin vous avait déjà faites. C'est une perte de temps et d'argent et les erreurs médicales sont plus grandes. Les données ne sont non plus pas uniformes, certains les stockent au format papier et d'autres au format électronique. De plus, cela empêche ou rend difficile l'échange des informations entre les différents acteurs du domaine de la santé.

Le dossier électronique du patient va regrouper l'ensemble des données médicales, de soins et administratives. Cet outil comprendra aussi le dossier de santé (dossier médical) qui contient des résultats d'analyses médicales, des rapports d'hospitalisation et des données numériques de toutes sortes d'examens. Son contenu sera donc très confidentiel.

Pour pouvoir accéder au dossier électronique du patient, le personnel médical devra avoir un accès réglementé. Ces droits seront accordés par le patient. La question que l'on se pose encore est la suivante : est-ce que les patients feront confiance et

accepteront d'avoir leurs données médicales dans une base de données centralisée ? Dans l'affirmative, le projet aura atteint un de ses objectifs.

TA-SWISS a fait un sondage (Publifocus), au printemps 2008, auprès de plusieurs personnes choisies au hasard en Suisse pour savoir ce que pensent ces futurs détenteurs du dossier électronique du patient (voir 2.6.5 - p.35). Les thèmes sensibles discutés portaient sur le respect de la sphère privée du patient, la vulnérabilité des données et leur utilisation.

Certaines personnes pourraient se sentir offensées de voir le médecin caché derrière son ordinateur et consulter ses données privées sur Internet au détriment d'un dialogue.

Les résultats du sondage effectué par TA-SWISS apparaissent plutôt satisfaisants étant donné que les participants sont favorables au dossier électronique. Ils proposent même d'inclure toutes les informations médicales depuis leur naissance jusqu'à aujourd'hui. Ils ne se rendent sûrement pas compte du travail que cela nécessite mais cela au moins montre leur confiance. Le problème de la sécurité des données se trouve à un autre niveau, on craint que les assurances ou les employeurs abusent de cet accès.

2.6.6. Dossier patient intégré (DPI) aux HUG

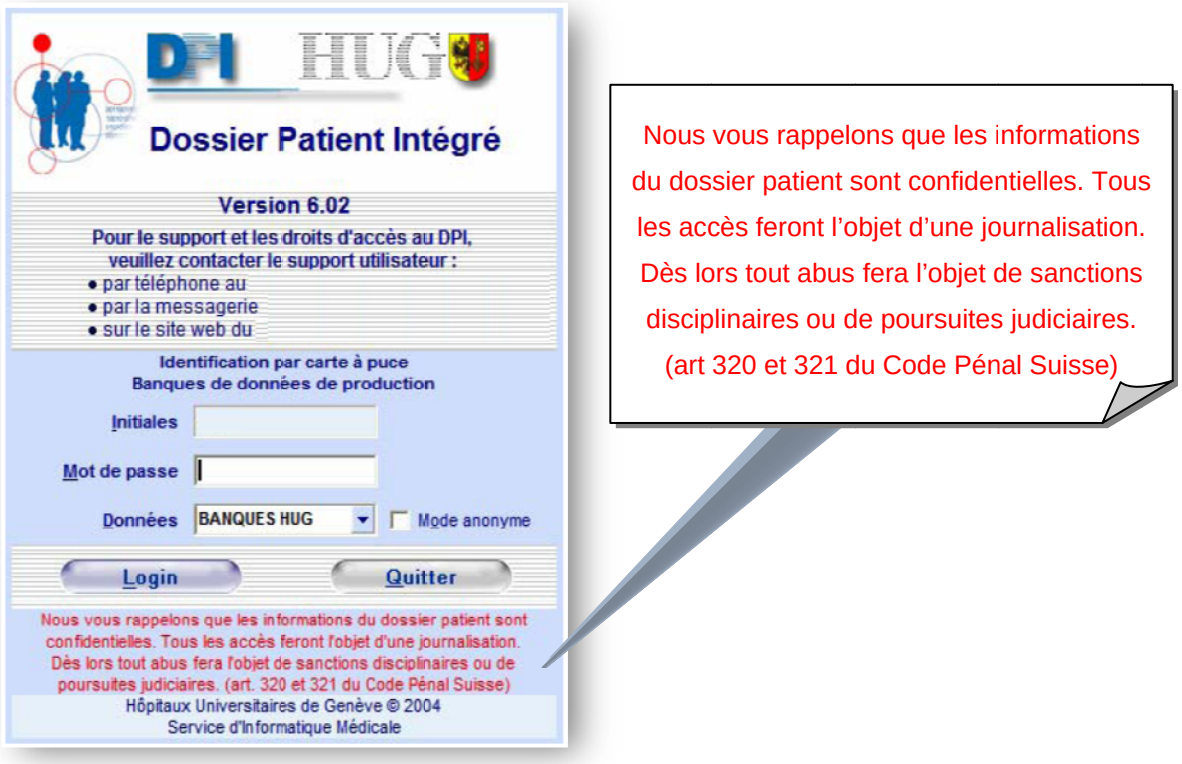
Le DPI est le dossier médical des patients pour tous les HUG. Cet outil comprend plusieurs modules : module médical, infirmier ainsi que des modules spécialisés. Les données ne sont accessibles qu'au personnel médical des HUG et des profils sont définis. Un profil infirmier étudiant ne verra pas autant d'informations qu'un profil infirmier. Voir Annexe 4, page 108 pour la liste des profils et leurs droits d'attribution.

La Figure 27 montre la page d'accès au DPI. Il faut évidemment une carte à puce pour pouvoir se loguer.

Figure 26
Carte à puce des employés HUG

Source : C. Lovis

Figure 27
Page d'accès au Dossier Patient Intégré



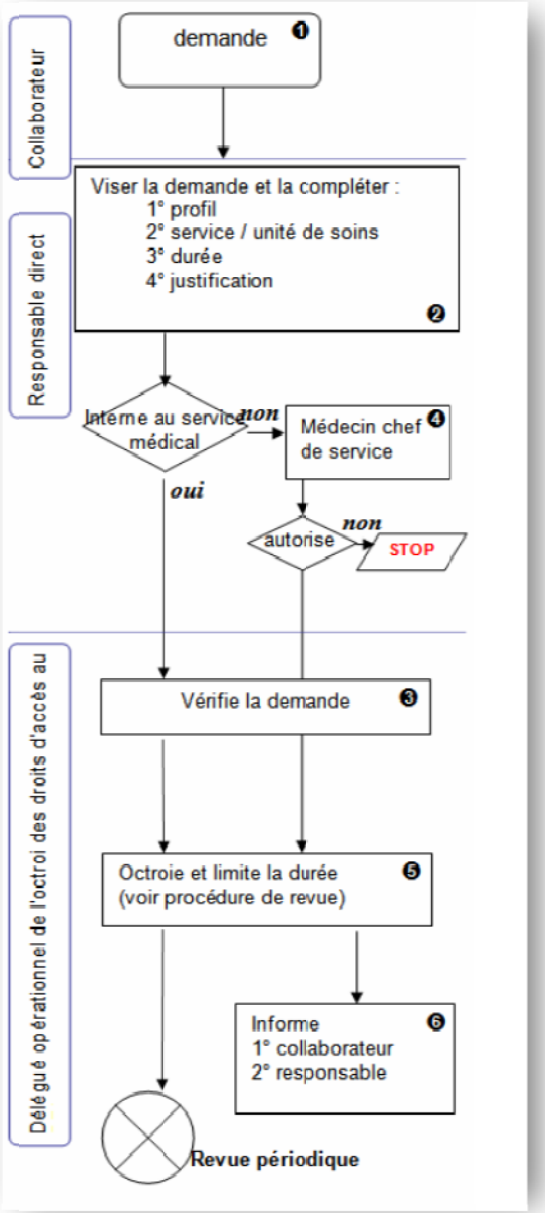
Source : Dossier patient, droits d'accès (p.6)

La gestion des droits d'accès.

Un groupe travaille sur les droits d'accès est supervisé par un comité de surveillance des accès informatiques. C'est le médecin chef qui octroi les profils qui ne sont attribués qu'à des employés avec un contrat actif. Les profils ont une durée limitée, normalement celle du contrat.

Figure 28

Demande de droits d'accès



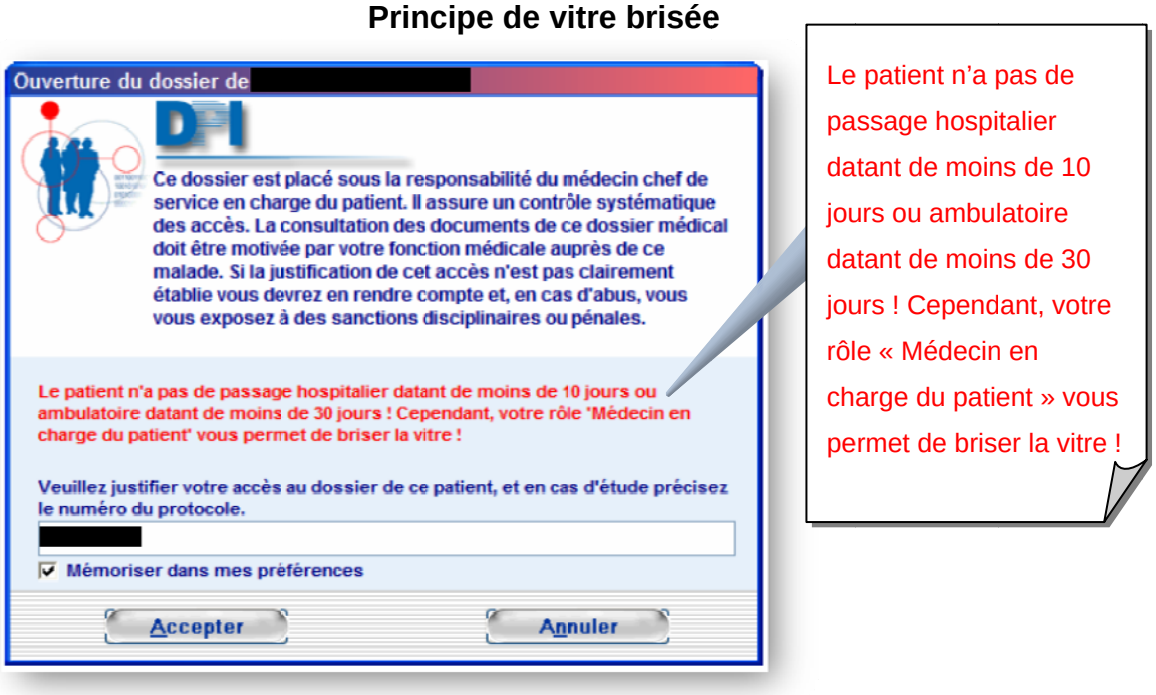
Source : Dossier patient, droits d'accès (p.16)

Principe de la vitre brisée

Ce principe permet à une personne n'ayant normalement pas le droit d'accéder à un dossier ou une partie de dossier d'y avoir exceptionnellement accès; pour cela une justification doit être fournie. Les manipulations sont enregistrées dans des journaux (log) et contrôlées par la suite (voir Figure 30).

Figure 29

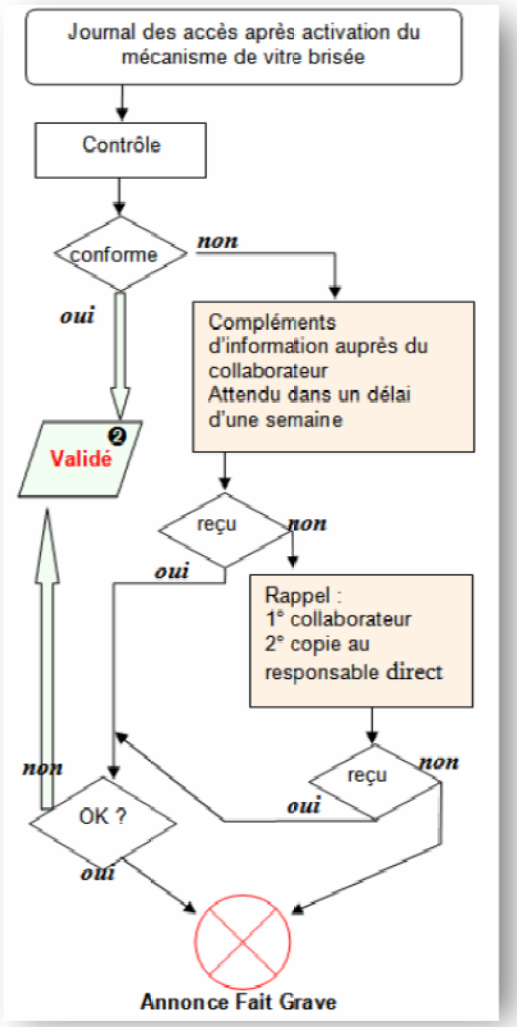
Principe de vitre brisée



Source : Dossier patient, droits d'accès (p.21)

Figure 30

Surveillance d'accès après le principe de vitre brisée



Source : Dossier patient, droits d'accès (p.24)

2.6.7. Carte d'assuré

Les données figureront directement sur la carte d'assuré et seront accessibles au moyen d'un code PIN[20] comme pour les téléphones portables ou les cartes bancaires. Les données permettront d'identifier le détenteur grâce aux informations administratives telles que le numéro d'assurance sociale qui sera stocké sur la carte; son but est de diminuer le travail administratif et standardiser la communication entre le corps médical et les assureurs. Par ailleurs les données médicales ne seront pas obligatoires et le patient pourra décider de les inclure ou non.

20 Code confidentiel

Si le patient décide de mettre ses données médicales sur cette carte, cela pourra peut-être lui sauver la vie. Par exemple, si un jour il se trouve dans une situation critique et est dans l'impossibilité de parler, sa carte, qu'il doit porter toujours sur lui, donnera les informations sur sa santé et le bon traitement pourra ainsi être prodigué.

2.6.7.1. Ordonnance électronique

L'ordonnance électronique permettra la prescription de médicaments directement avec les pharmacies et automatisera le processus de facturation. Elle améliorera la gestion de prises de médicaments qui est souvent un problème surtout pour les personnes âgées qui se voient prescrire des médicaments contradictoires par plusieurs médecins.

2.6.7.2. Télémédecine

Un service de télémédecine offrirait au patient la possibilité d'entrer en contact avec un médecin via Internet, par écrit, ou par téléphone. Cela permettrait de faire un premier diagnostic et d'éviter des consultations qui ne sont pas nécessaires.

2.6.8. Carte professionnelle de santé

La **C**arte **P**rofessionnelle de **S**anté (CPS) ou **H**ealth **P**rofessional **C**ard (HPC) en anglais est détenue par un professionnel de la santé. Elle permet de l'identifier et lui laisse l'accès aux données auxquelles il a le droit. (Voir Figure 26 page 45 comme exemple).

Source : http://www.saez.ch/pdf_f/2007/2007-38/2007-38-891.PDF

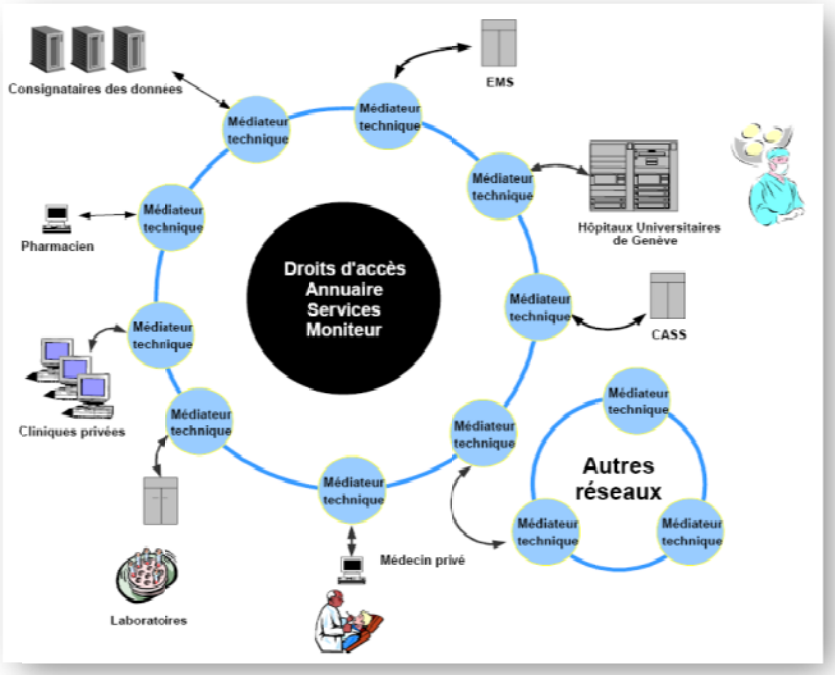
Figure 31
HPC

Source : http://www.hpcsystem.ch/frn/HPCNewsFR_200403.pdf (p.2)

2.6.9. Projet e-Toile

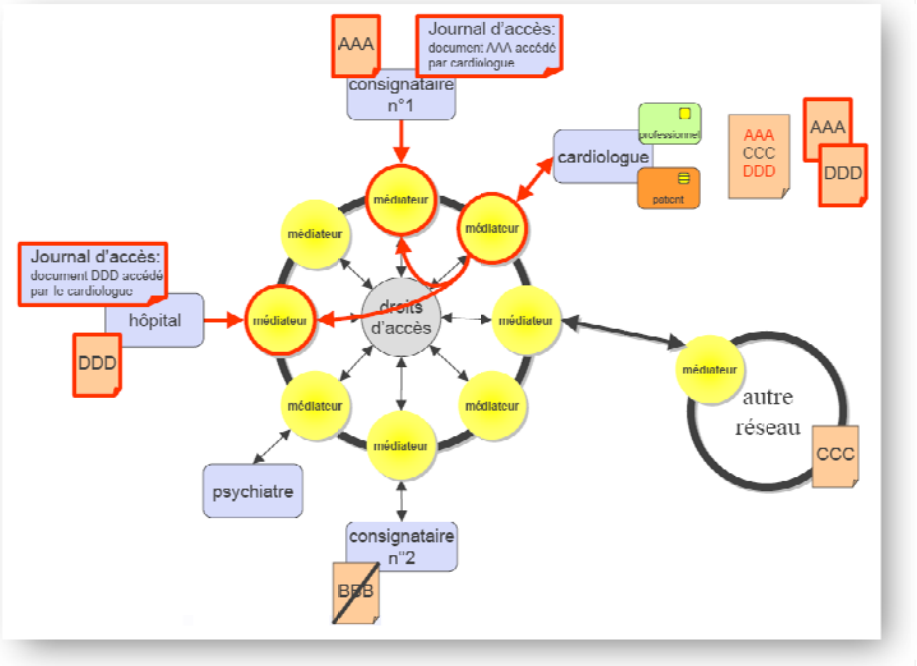
e-Toile est un projet genevois qui a vu le jour il y a plus de 8 ans. Contrairement à d'autres projets, celui-ci ne veut pas réunir les informations dans une base de données centralisée. Chaque entité de soins qui voudra accéder à des renseignements passera par l'organe e-Toile et en fera la demande aux entités de soins possédant les données (voir Figure 32 et Figure 33).

Figure 32
Architecture du réseau e-Toile



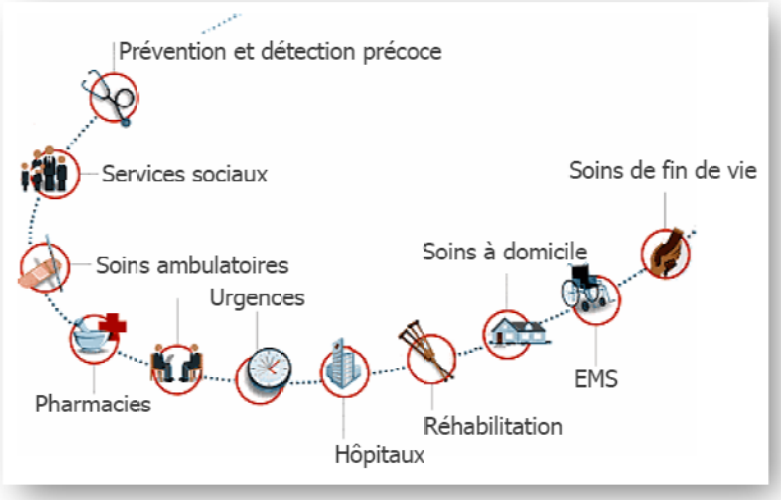
Source :
http://etat.geneve.ch/des/SilverpeasWebFileServer/iris_rapport.pdf?ComponentId=kmelia518&SourceFile=1125050473318.pdf&MimeType=application/pdf&Directory=Attachment/Images/&logicalName=iris_rapport.pdf

Figure 33
Architecture et exemples



Source : http://www.ta-swiss.ch/a/info_tele/041102_RE_geissbuhler_f.pdf (p.23)

Figure 34
Partenaires e-Toile



Source : Un projet de réseau communautaire d'informatique médicale (p.8)

Partenaires :

- 450'000 citoyens
- 1'400 médecins privés
- 1'000 soignants à domicile
- 6'000 médecins et infirmiers dans les hôpitaux publics
- 51 établissements de long séjour
- 12 cliniques privées
- 150 pharmacies
- 10 laboratoires d'analyses
- Physiothérapeutes, dentistes, spécialistes…

2.6.10. Projets dans d'autres cantons

Lugano a lancé un projet pilote en 2004 avec la carte de santé à puce électronique; cela a été une réussite à tel point que la protection des données n'a plus été au cœur du sujet.

Saint-Gall va instaurer d'ici à 2010 l'échange de données électroniques des patients via un réseau entre les établissements du canton.

Lucerne a mis en place l'échange de données électroniques entre les entités de soins du canton et d'autres hôpitaux ainsi que les médecins de famille.

2.6.11. Standards et interopérabilité

Des standards existent pour permettre l'échange de données de façon homogène et permettre l'interopérabilité entre les différents acteurs.

2.6.11.1. HL7

Health **L**evel **7** (HL7) est un standard d'échange de fichiers médicaux. Le « 7 » signifie qu'il travaille au niveau 7 de la couche OSI[21] (couche application qui accède aux réseaux). Le HL7 est aujourd'hui utilisé mais pour les applications intra-hôpitaux,

21 Modèle de communication entre ordinateurs selon la norme ISO

notamment aux HUG. La sémantique ressemble à celle du langage XML[22] de par ses balises.

2.6.11.2. CDA

Clinical **D**ocument **A**rchitecture (CDA) n'est pas un protocole de communication mais un protocole d'échanges d'informations médicales qui est défini par le HL7.

2.6.11.3. DICOM

DICOM est un standard de communication en imagerie médicale. Il est surtout utilisé en radiologie mais également en cardiologie, pour la médecine vétérinaire, la radiothérapie, l'ophtalmologie etc.

Figure 35
Image de médecine nucléaire au format DICOM

Source : http://fr.wikipedia.org/wiki/DICOM

2.6.11.4. CUMUL

CUMUL est un projet de répertoires des analyses cliniques, version « Suisse » du LOINC qui lui vient des Etats-Unis. Il rend possible l'échange de données entre les entités de soins de façon hétérogène. Le site cumul.ch permet de télécharger un fichier

22 Langage informatique de description de documents en le structurant de façon standard

Access[23] qui comporte des tables avec les codes CUMUL. Il est néanmoins interdit de créer ou de modifier un champ de la table et encore moins d'en détourner son sens. J'ai moi-même ouvert ce fichier et constaté que toutes les modifications, même involontaires, sont réalisables…

*« Le **C**entre **S**uisse de **C**ontrôle de **Q**ualité (CSCQ) ne formule aucune garantie et n'est engagé par aucune erreur ou omission dans la base de données CUMUL et écarte toute prétention à réclamation quant aux fonctions exprimées ou implicites des données, que leurs implications soient commerciales ou de toute autre nature. »*

2.6.11.5. LOINC

Logical **O**bservations, **I**dentifiers, **N**ames, and **C**odes (LOINC) est un répertoire, référentiel des analyses cliniques.

Source : http://www.cumul.ch/4_dld_fr.htm

2.7. Pour ou contre ?

J'ai posé des questions à des connaissances travaillant dans le domaine médical et voici leurs avis sur le sujet.

*« Dans une partie des HUG, on utilise un dossier patient informatisé (DPI MI = **D**ossier **P**atient **I**ntégré **M**odule **I**nfirmier). Tout l'hôpital n'est pas encore sur ce type de dossier mais c'est en train d'être généralisé.*

*Pour des raisons pratiques, d'écritures et pour accéder aux données concernant un patient, **je trouve le dossier informatisé super**. Mais pour y accéder il faut un badge, muni d'une puce et on doit entrer ses initiales puis un mot de passe. En tant qu'infirmière, on a aussi accès au dossier médical informatisé. Il y a également un logiciel concernant les ordres médicaux informatisés, mais il n'est pas encore partout en vigueur dans les HUG.*

Par rapport à ceci, il faut savoir que tous les soignants sont tenus au secret médical et au respect de la confidentialité des données. (C'est dans la loi). Donc je n'ai pas peur pour la sécurité de ces données car elles sont exclusivement

23 Outil Microsoft de bases de données

réservées à l'équipe soignante, mais il est vrai qu'on a plus facilement accès aux dossiers de patients d'autres unités par exemple.»

Laurence GROUX, infirmière aux HUG

« Je travaille actuellement à la FSASD (soins à domicile). Lorsque je travaillais à l'hôpital de la Tour de Genève, nous n'avions pas le dossier informatisé.

Actuellement tous nos dossiers patients sont avant tout sur support papier; nous ne sommes pas informatisés comme aux HUG par exemple. Nous avons tout de même ce que l'on appelle un Pocket PC, petit ordinateur qui nous permet d'établir et d'imprimer nos plans de soins pour chaque patient. Ce système est très sécurisé dans le sens où chaque infirmière possède un code personnel d'accès et que nous pouvons actualiser nos données qu'au bureau à l'aide d'une borne de synchronisation wifi[24].

Je pense que pour une question de rapidité administrative ***cette méthode est favorable****, en tout cas j'y suis favorable.* ***Quant à la sécurité des données, j'ai effectivement des doutes; lorsqu'on voit que des petits génies de l'informatique accèdent aux données top secrètes de Davos par exemple, cela me laisse sceptique...***

Pour ma part je pense qu'il faut garder deux systèmes de support : papier plus informatique. Mais les données écrites peuvent également être insécurisées en cas de vol de dossiers par exemple. Mais à mon avis cette dernière hypothèse est plus rare. Il me paraît plus évident de rentrer par effraction dans un système informatique. Donc il s'agit de savoir quelles données nous allons y mettre. »

Lisa GAUTSCHI infirmière à la FSASD

Quant à José Campos, médecin orthopédiste aux HUG, il est favorable au DPI (**D**ossier **P**atient **I**ntégré) qu'il utilise déjà. Il trouve que c'est un **gain de temps et d'énergie** et la **sécurité des données ne l'inquiète pas**.

24 Connexion réseau sans fil

3. Qu'existe-t-il à l'étranger ?

Les lois ne sont pas tout à fait les mêmes à l'étranger qu'en Suisse c'est pourquoi nous ne pouvons pas comparer les projets et les technologies qui se font hors de nos frontières. Je vais tout de même présenter ce qui existe ailleurs car cela arrivera peut-être un jour ici.

3.1. VeriChip

VeriChip est une puce électronique, pas plus grande qu'un grain de riz (voir Figure 36), de la société Applied Digital, que l'on implante sous la peau comme les puces électroniques des animaux. Le composant a un identifiant unique de 16 chiffres qui peut être lu à distance avec un lecteur de données (voir Figure 37 et Figure 38). Cette technologie est basée sur le RFID (**R**adio **F**requency **I**dentification **D**evices), en français, dispositif d'identification par onde radio.

Aux Etats-Unis, depuis 2002, il est possible de se faire implanter la VeriChip, cette puce électronique pour seulement 200$. Elle fonctionne comme nos GPS et nos portables, par antennes relais.

Nous possédons tous une carte à puce RFID, elle se trouve sur notre carte de crédit, dans notre ordinateur... Certains magasins mettent ces « mouchards » sur leurs produits à des fins de marketing, par exemple, pour pouvoir gérer les stocks automatiquement ou étudier les habitudes des consommateurs.

Certaines personnes disent qu'il y aurait un risque de manipulation du comportement du détenteur de la puce. Des études montrent que certaines impulsions peuvent par exemple toucher les neurotransmetteurs, ce qui aurait pour conséquence une possible manipulation dans des idées politiques ou autres. Par exemple, en intensifiant les ondes, on peut produire de l'adrénaline et de ce fait modifier un comportement, ou créer plus ou moins d'hormones et ainsi contrôler la natalité d'un pays.

Figure 36
Puce électronique VeriChip

Source : http://www.jpn-online.ch/JPN-online/archives_news/VeriChip01.jpg

Figure 37
Lecteur optique

Figure 38
Portillon lecteur optique

Source : http://www.freewebs.com/nomicrochip/

Avantage :

Imaginons que vous faites un malaise et que vous êtes diabétique, les informations qui seront lues sur votre puce indiqueront que vous avez besoin d'une piqûre d'insuline et cela très rapidement; sans devoir attendre l'arrivée aux urgences, votre vie pourra ainsi être sauvée.

Désavantage :

On pourrait imaginer que les assurances arrivent à scanner votre dossier et refusent de vous assurer à cause de votre passé médical trop lourd à leurs yeux. Un patron veut vous engager mais grâce à la puce qu'il pourrait scanner (de façon illégale bien sûr), il constaterait que vous avez été en congé maladie quelques années auparavant pour une dépression. Ne pensez-vous pas qu'il préfèrera engager quelqu'un moins sujet à cette maladie et qui risque de connaître moins d'absentéisme ?

Ou pire, un scénario digne d'un film d'horreur. On ne sait jamais de quoi l'être humain est capable, les guerres nous ont prouvé que l'on peut s'attendre à tout. Imaginons que des personnes contaminées par une maladie soient identifiables par une micro-puce implantée dans leur corps et qu'elles puissent être interdites d'accès aux lieux publics, dans les magasins… Cette technologie peut aller vraiment loin, à nous de la maîtriser.

3.2. Carte Vitale

En France, la carte vitale permet à son titulaire de disposer d'une couverture sociale. Elle stocke les données personnelles comme le numéro d'assuré, l'identité de la personne et sa caisse de sécurité sociale.

Source : http://www.zataz.com/communique-presse/15647/La-nouvelle-Carte-Vitale-2-passe-par-FIME.html

3.2.1. De gros problèmes de sécurité

En 2005, un informaticien a démontré qu'il existait des failles dans la carte vitale 1, on pouvait notamment utiliser de fausses cartes d'assurés, en dupliquer et même en créer de nouvelles. Au début, cet informaticien n'a pas été entendu et, pour attirer l'attention sur ce danger, il a créé une fausse carte et s'est fait délivrer des médicaments par deux pharmacies pour plusieurs centaines d'euros. Dès ce moment là, les responsables ont commencé à prendre cette histoire au sérieux et ont promis que les problèmes seraient réglés dès le 2e semestre 2006. Mais n'était-ce pas un peu tard ?

Source : http://www.telemedecine.org/article.php?sid=952

3.2.2. Carte Vitale 2

La carte vitale 2 va remplacer d'ici 2010 la carte vitale 1 qui n'était pas sécurisée et ne proposait pas assez de place pour les données. Des tests plus poussés vont être effectués pour s'assurer d'une meilleure sécurité. Ces tests se feront sur les bornes de mise à jour, sur les terminaux de lecteurs qui sont chez les médecins, sur la calculette de lecture de carte et sur les dispositifs intégrés dans les systèmes des pharmacies.

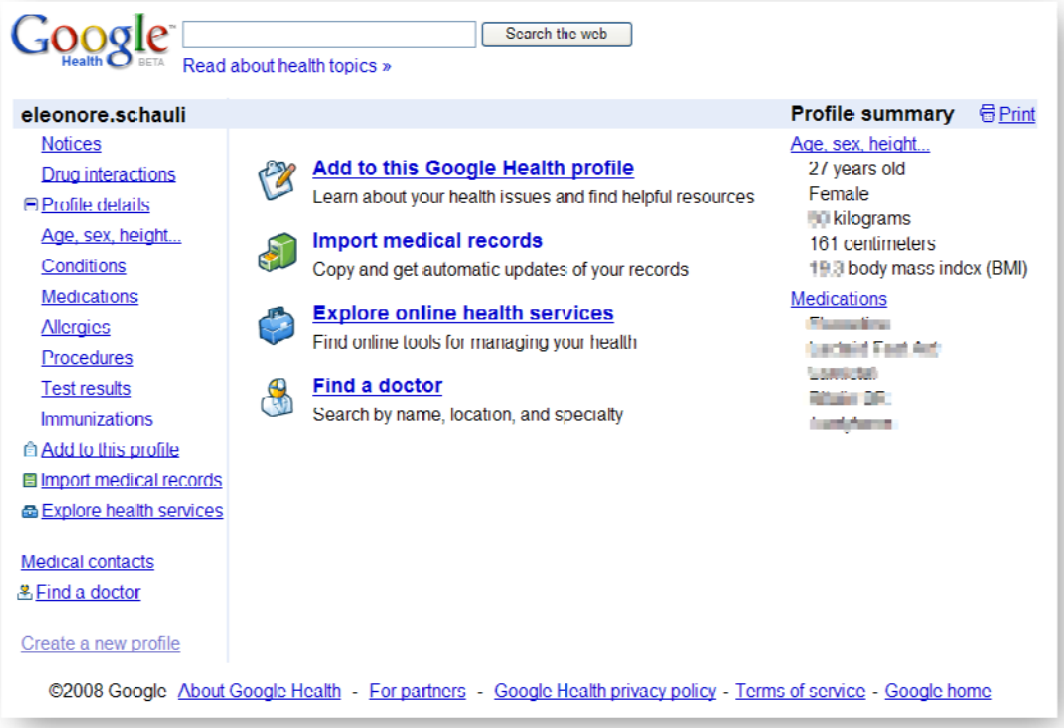
Figure 39
Carte Vitale 2

Source : http://www.siteduzero.com/uploads/fr/files/49001_50000/49893.png

3.3. Google Health

La célèbre société Google vient de lancer « Google Health » qui propose gratuitement depuis mars 2008 un espace de stockage et d'archivage de données médicales sur Internet. On appelle une telle plateforme un PHR (**P**ersonal **H**ealth **R**ecord), en français : dossier personnel de santé. Il n'existe, à l'heure actuelle, qu'en version Beta[25]. Les lois appliquées sont évidemment celles des Etats-Unis. Après l'ouverture d'un compte chez Google, l'internaute (le patient) crée son propre carnet de santé virtuel qu'il est le seul (en théorie) habilité à modifier. Le mot de passe est le même que celui utilisé pour la boîte e-mail de Google, Gmail. Le patient peut donner des droits à des personnes ou des instituts médicaux afin de consulter ce dossier médical.

Figure 40
Mon PHR Google Health



Source : https://www.google.com/health/p/

Google propose encore davantage : suivant la pathologie du patient, une liste de médecins spécialisés est proposée. Il est aussi mis en garde si des médicaments qu'il prend ne sont pas compatibles entre eux.

25 Version de test

Et la sécurité dans tout ça ? Google garantit les données par un mot de passe. Des chercheurs américains se sont penchés sur la question et ont remarqué des faiblesses. Google est connu pour ses problèmes de sécurité.

La société Privacy International[26] a mené une enquête durant 6 mois sur une vingtaine de sites Internet qui stockent des données personnelles et Google a fini dernier du classement.

Tableau 3

Analyse de Google par Privacy International

Google	
Détails administratifs	Privacy Matters, c/o Google Inc, 1600 Amphitheatre Parkway, Mountain View CA 94043 (USA).
Collecte et traitement des données	Les adresses IP[27] ne sont pas considérées comme des renseignements personnels. Google analyse les liens cliqués.
Conservation des données	Imprécis mais environ 18 à 24 mois. L'historique est conservé après cette période.
Ouverture et transparence	La politique de confidentialité est vague, incomplète et trompeuse. Les chartes n'expliquent pas le traitement des données détaillées des éléments ou des flux d'information.
Repères éthiques	Le mandat de la vie privée n'est pas inclus dans l'ensemble de la société. Les techniques et les technologies sont souvent déployées sans une consultation du publique.
Contrôle des clients	Les clients ont le droit de modifier les informations personnelles détenues par Google, mais ne peuvent pas supprimer l'historique.
Navigation	Certain services peuvent ne pas fonctionner sans l'activation des cookies[28].
L'amélioration de la vie privée ou l'invasion de l'innovation	Utilise la publicité profilée selon les liens cliqués sur la page web.
Évaluation initiale	Surveillance complète du consommateur.

Source : traduit de http://www.privacyinternational.org/issues/internet/interimrankings.pdf

26 Organisation de défense de la vie privée

27 Numéro qui identifie un ordinateur connecté à Internet

28 Fichiers textes qui recensent des informations sur la navigation sur site Internet

« Google n'est pas soumis aux vérifications de conformation à l'HIPAA (**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct) qui permettent de s'assurer du respect de la confidentialité des données médicales personnelles. »

Source : http://www.jbkempf.com/blog/post/2008/05/29/Gestion-des-dossiers-medicaux-par-Google-Health

Bien qu'il soit de notre devoir de lire les termes d'un contrat, nous sommes nombreux à ne pas le faire et sommes donc dans notre tort. Analysons ci-dessous ce que dit Google et voyons si leurs conditions sont satisfaisantes.

3.3.1. Traduction des conditions de Google Health

« 3. Votre compte et l'utilisation de Google Health

Vous devez fournir des informations d'enregistrement précises et complètes à chaque fois que vous utilisez Google Health. ***Vous êtes responsable de la sécurité de vos mots de passe et pour toute utilisation de votre compte.*** *Vous devez immédiatement informer Google de toute utilisation non autorisée de votre mot de passe ou de votre compte.*

…

Votre utilisation de Google Health et tout le contenu accessible par l'intermédiaire de Google Health doit se conformer à toutes les lois, règlements et ordonnances, y compris les lois concernant l'exportation de données ou de logiciels. Vous devez avoir au moins 18 ans pour utiliser Google Health. »

« 4. L'utilisation de vos informations

Si vous créez, transmettez ou affichez des informations médicales ou d'autres informations lors de l'utilisation de Google Health, ***vous devez seulement fournir les informations que vous possédez ou que vous avez le droit d'utiliser.*** *Lorsque vous fournissez vos informations médicales par le biais de Google, Google vous donne une licence pour l'utilisation et la distribution en ce qui concerne Google Health et d'autres services Google.* ***Toutefois, Google Health doit seulement utiliser vos informations dans la mesure permise par la politique de confidentialité de Google Health, le partage que vous avez autorisé, et la loi applicable.*** *Google n'est pas une «entité visée» en vertu de l'assurance maladie et la portabilité Accountability Act de 1996 et les règlements*

promulgués à ce titre ("HIPAA"). En conséquence, HIPAA ne s'applique pas à la transmission de l'information par Google Health à un tiers. »

« 6. Le contenu et les services accessibles via Google Health

…

Google se réserve le droit de faire appel à des tiers. ***Pour l'utilisation d'un service spécifique, vous devez permettre au tiers (fournisseur de services), d'obtenir, fournir et/ou de modifier des informations médicales et d'autres informations de votre compte ou de partager vos informations avec le fournisseur de services.*** *Une fois que vous acceptez d'activer un tiers fournisseur de services à accéder à votre compte, il doit pouvoir continuer à le faire jusqu'à ce que vous décidiez de désactiver l'accès. Ces tiers peuvent être des fournisseurs de soins de santé ou d'autres entités.* ***Il est de votre seule responsabilité d'examiner et d'approuver chacun de ces services tiers avant de partager vos informations par le biais du site.***

…

L'utilisation de ces services et la fiabilité de leur contenu se fait à vos risques et périls. Google ne peut pas être tenu responsable en cas de dommage survenant lors de l'utilisation de services tiers. »

Source : traduit de http://www.google.com/intl/fr-CH/health/terms.html

3.3.2. Autorisation

*« **J'autorise Google à partager les informations médicales figurant dans mon profil Google Health dans leur intégralité, avec les seuls entités et individus que j'ai désignés,** dans le but de me prodiguer des soins médicaux et de partager mes informations avec les personnes de mon choix.*

Je comprends et j'accepte que cette autorisation permet la divulgation d'informations concernant ma santé, ou des traitements dont je fais l'objet, à des entités et des personnes que j'ai désignées; je suis conscient que ces données pourraient contenir des informations sensibles.

…

Je comprends et j'accepte que cette autorisation se rapporte également à tout document émis par un médecin ou un fournisseur de soins de santé

autres que le médecin ou le prestataire de soins qui a fourni le dossier à Google Health.

Cette autorisation restera en vigueur et permettra la divulgation des informations en cours par Google dans le service de Google Health jusqu'à ce que je supprime entièrement mon profil dans Google Health ou révoque l'autorisation.

…

Je comprends que ma révocation ne s'applique pas aux actions que Google a déjà prises en rapport avec mon autorisation préalable.

Je comprends et accepte que, outre les données que j'ai choisi de partager, Google ne peut divulguer l'information que dans les circonstances limitées décrites dans la politique de confidentialité de Google Health. »

Source : traduit de http://www.google.com/intl/fr-CH/health/sharingauth.html

3.3.3. Centre d'aide Google Health

La suppression des données

« Des copies des données stockées dans Google Health peuvent persister jusqu'à 30 jours après que les données aient été supprimées. Après ce délai, elles sont totalement supprimées. »

Source : traduit de http://www.google.com/support/health/bin/answer.py?answer=94515&topic=14631

4. La sécurité des systèmes d'information

Dans ce chapitre, je souhaite aborder les sujets qui traitent de la sécurité et des divers protocoles énumérés dans les précédents chapitres.

Avec la « sécurité des systèmes d'information » on cherche à protéger l'**intégrité**, la **confidentialité** et la **disponibilité** des données. Ces trois termes reviennent tout le temps dès que l'on parle de la sécurité. Pour sécuriser ces données on va procéder à des méthodes de chiffrement.

Le but est que seules les personnes autorisées aient accès à l'information. Mais comment être sûr que le destinataire est bien le bon ? Pour cela, il existe plusieurs méthodes et algorithmes que je vais expliquer ci-dessous. On utilise aussi des certificats; il y a justement des « entités » ou tierces personnes morales qui sont accréditées pour certifier les canaux d'échanges. Ces certificats sont utilisés par exemple par les médecins et les unités de soins qui veulent transférer des informations confidentielles en « toute » sécurité.

4.1. Politique de sécurité

Pour instaurer une bonne politique de sécurité, il faut faire au préalable une analyse des risques. Son résultat permettra de mettre en place une politique de sécurité adéquate au système à protéger. Les objectifs de la sécurité informatique sont les suivants :

Disponibilité :

- Il s'agit de rendre les données disponibles à tout moment.

Intégrité :

- Les données que l'on reçoit doivent être celles que l'on croit recevoir et ne doivent pas avoir été altérées durant la transaction.

Confidentialité :

- Seules les personnes ayant droit à ces données doivent pouvoir y accéder.

Non-répudiation :

- La garantit qu'une transaction ne peut être niée.

Authentification :

- Assure l'identité de l'utilisateur et garantit à l'interlocuteur que la personne en face est bien la bonne.

4.2. Les hackers

Qui sont ces personnes qui veulent attaquer un système informatique ? On les classe en plusieurs catégories. Il y a d'abord les **curieux** qui, intentionnellement ou non, s'introduisent dans un réseau et ont accès à des données confidentielles. Ils ne créeront généralement aucun dommage, ils aiment juste fouiller dans les affaires des gens. Ensuite, l'**ingénieux**, appelé « geek » dans le jargon informatique, est le passionné qui se prend pour un génie lorsqu'il réussit à craquer un réseau. Il n'a aucun intérêt pour les informations qu'il découvre mais ce qui l'intéresse c'est d'avoir réussi à y accéder. Enfin, le **professionnel** : on parlera de « taupe » car il agira à des fins commerciales ou frauduleuses, le terme exact de ses agissements s'appelant l'ingénierie sociale. Les menaces peuvent être structurées ou non, internes ou externes à l'entreprise.

4.3. Les failles

Les plus grands problèmes dans la sécurité informatique ne proviennent pas du piratage, ni des attaques ou des virus, mais sont le fait de l'être humain qui fait de mauvaises manipulations, perd des données importantes ou se fait voler son matériel. La sécurité au niveau purement informatique est généralement bonne mais l'utilisation que les gens en font la rend vulnérable.

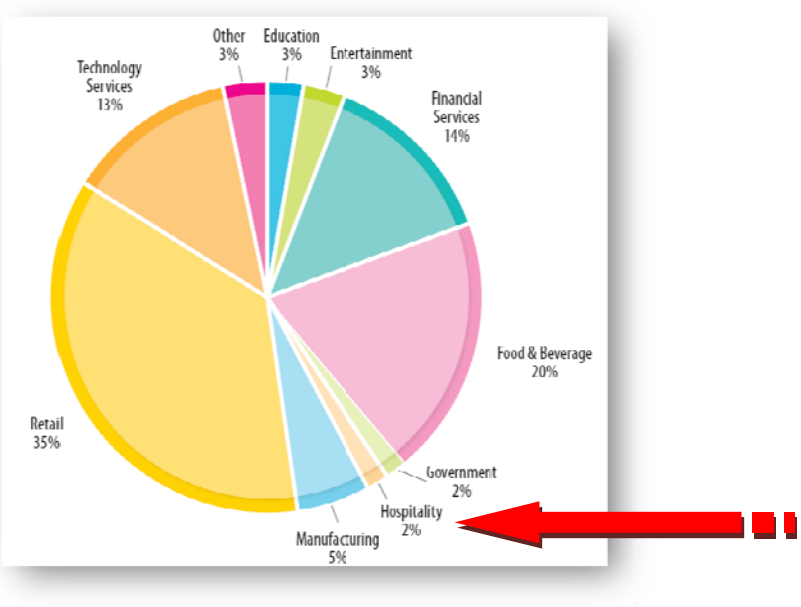
Souvent les gens inscrivent leurs mots de passe sur un bout de papier afin de ne pas les oublier mais, une fois écrits, ils deviennent accessibles à tout le monde. Sans parler des personnes qui utilisent le nom de leur animal, la date de naissance de leur enfant ou leur numéro de téléphone ! Bien que la sensibilisation aux utilisateurs soit faite, c'est encore trop souvent que l'on trouve des mots de passe si mal protégés.

Une bonne campagne de sensibilisation peut réduire les problèmes de sécurité liés à l'erreur humaine.

Une étude publiée par Verizon montre que seulement 2% des failles touchent le secteur hospitalier. Elle a été effectuée sur 4 ans avec un échantillon de 500 entreprises.

Source : http://www.pcinpact.com/actu/news/46486-entreprises-securite-breches-protocoles.htm

Figure 41
Pourcentage de failles par secteur



Source : http://www.verizonbusiness.com/resources/security/databreachreport.pdf (p.8)

4.3.1. Les erreurs humaines

Les risques humains sont les plus importants et cependant souvent banalisés. On peut les classer en plusieurs catégories. Même les personnes bien informées peuvent devenir une menace. La **négligence ou l'ignorance** par exemple peuvent presque être associées à un acte volontaire.

Exemples au travail :

- On est vendredi soir, vous êtes fatigué et vous voulez rejoindre votre famille alors vous omettez de faire la sauvegarde qui est normalement la procédure à exécuter en fin de semaine…
- Votre anti-virus prend trop de temps et vous êtes pressé d'aller manger, vous éteignez l'ordinateur alors que le processus n'est pas terminé…

- Vous êtes malades et votre patron a vraiment besoin d'un dossier qui se trouve dans votre ordinateur. Comme vous ne voulez pas vous déplacer et que vous lui faites confiance, vous lui donnez votre mot de passe…
- Bien que cela soit interdit, vous installez un logiciel qui vous permet de chatter[29] avec vos amis…
- Vous renversez votre verre d'eau sur votre ordinateur…

L'**incapacité ou la maladresse** d'une personne devient malheureusement une menace bien qu'elle ne soit pas intentionnelle.

Exemples au travail :

- Ne voyant pas à quoi servent certains fichiers, vous décidez de les effacer…
- Votre doigt glisse sur la touche « Delete[30] » ou tout simplement vous faites une erreur de manipulation en envoyant le mauvais fichier à la poubelle…
- Vous recevez un appel du technicien qui doit venir faire des réparations. Vous lui donnez l'architecture des locaux informatiques et des systèmes utilisés, pourtant aucun technicien n'avait été prévu… Cette méthode s'appelle « l'ingénierie sociale », il s'agit de se faire passer pour quelqu'un d'autre afin d'obtenir des informations confidentielles.

Lois de non-fiabilité de Gibbs

- *« Les ordinateurs ne sont pas fiables, les hommes le sont encore moins. À l'origine de chaque erreur attribuée à l'ordinateur, on trouve au moins deux erreurs humaines, dont celle qui consiste à accuser l'ordinateur.*
- *Tout système qui dépend de la fiabilité de l'homme n'est pas fiable.*
- *La seule différence entre un imbécile et un criminel qui attaque un système réside dans le fait que l'action de l'imbécile est imprévisible et d'une plus grande envergure.*

29 Discuter sur Internet

30 Touche « Supprimer » sur un clavier d'ordinateur

- *Il existe une quantité infinie d'erreurs non décelables, alors que le nombre des erreurs décelables est, ipso facto, limité.*
- *Les investissements pour assurer la fiabilité augmenteront jusqu'à ce qu'ils excèdent le coût probable des erreurs... ou jusqu'à ce que quelqu'un exige que l'on fasse du bon travail. »*

Source : http://archimede.mat.ulaval.ca/guide/node109.html

4.3.1.1. Comment s'en protéger ?

En faisant des campagnes de sensibilisation pour tous les employés et une formation sur la bonne utilisation des logiciels et des procédures.

Le CLUSIF (**CLU**b de la **S**écurité de l'**I**nformation **F**rançais) est un club qui accueille des entreprises ou des collectivités pour agir sur la sécurité des systèmes d'information. Il propose des formations, des documents, notamment des rapports relatifs à la sécurité et beaucoup d'autres choses que l'on peut consulter sur leur site. Le CLUSIS (**CLU**b de la **S**écurité de l'**I**nformation **S**uisse) est le partenaire helvétique du CLUSIF.

Le CLUSIF a créé une méthode d'analyse des risques nommée MEHARI (**ME**thode **H**armonisée d'**A**nalyse de **R**isques). Elle peut s'adapter à toutes sortes d'entreprises et donc être utilisée pour mettre en place des parades.

Le **C**omputer **E**mergency **R**esponse **T**eam (CERT) est un organisme qui s'occupe de centraliser les incidents et les erreurs informatiques et les rend accessible au publique.

4.3.2. Cas de failles

Un site Internet américain (dataloss db open security foundation) recense beaucoup de cas de failles qui se sont produits dans le monde. J'ai trouvé quelques exemples dans le domaine médical.

Les cas sont répertoriés par dates et on peut s'apercevoir qu'il y en a tous les jours ! Ils sont classés par secteurs : business, éducation, gouvernement et médical. La source est soit inconnue, extérieure, intérieure, intérieure et malicieuse ou intérieure et accidentelle. Un logo précise le type de brèche. Ensuite des détails sont donnés sur le cas ainsi que la localisation.

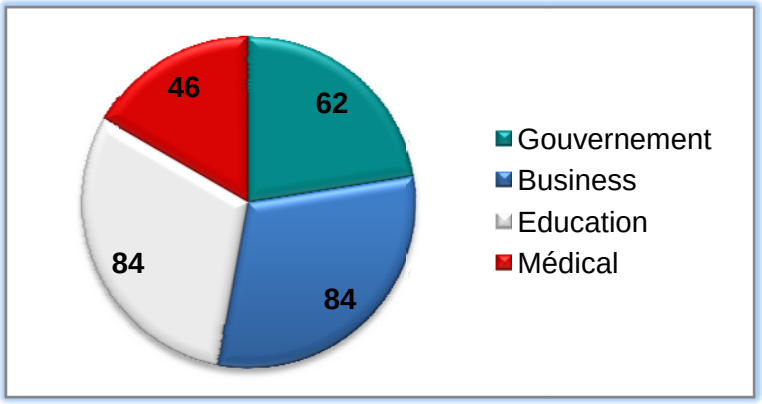
Un résumé précise si les données ont été retrouvées, en combien de temps, si des poursuites judiciaires ont été faites, qui a découvert la faille, quand et comment, etc.

Des liens avec des cas similaires sont disponibles sur la même page (voir Annexe 3 - p.107).

Il est intéressant de jeter un coup d'œil sur ce site pour constater que de nombreuses erreurs sont de nature humaine, notamment le vol d'ordinateurs portables (voir Tableau 4).

Figure 42

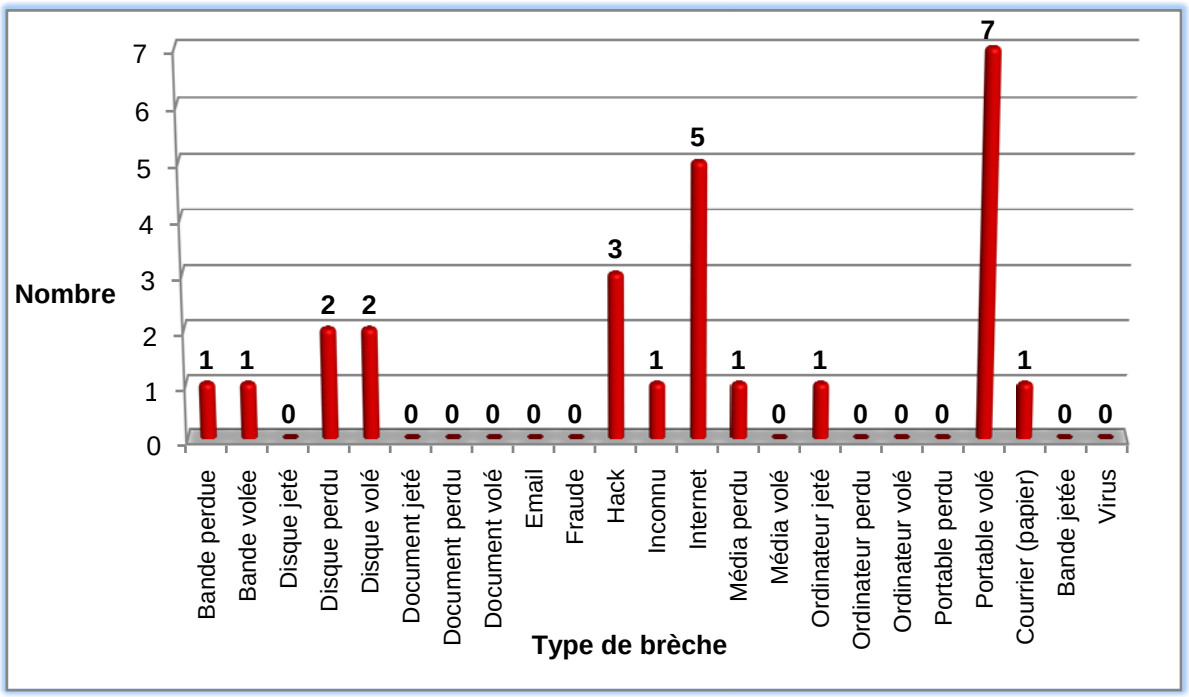
Nombre d'incidents par secteur entre janvier et juillet 2008



Source : http://datalossdb.org/yearly_reports/dataloss-2008.pdf

Tableau 4

Incidents entre janvier et juillet 2008 dans le milieu médical



4.4. La cryptographie

La cryptographie vient du mot cryptologie, science du secret. Elle englobe l'arithmétique, l'algèbre, la théorie de l'information, etc. Le premier document chiffré date du XVI^{e} siècle avant Jésus-Christ, il s'agissait d'une recette qui avait été gravée dans de l'argile. L'orthographe des mots et des voyelles avaient été changée. Elle a beaucoup été utilisée par les services secrets, par l'armée pendant les guerres avant d'être utilisée en informatique dans notre vie quotidienne.

4.4.1. Exemples de cryptogrammes

Ces méthodes sont dites de transpositions ou substitutions, cela signifie que les lettres sont permutées. Voici quelques exemples parmi beaucoup d'autres.

Le carré de Polybe. Chaque lettre correspond à 2 chiffres. Le code se construit avec le chiffre vertical suivi du chiffre horizontal.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Mot « Cryptogramme » crypté avec le carré de Polybe :

Cryptogramme → 13425435443422421132321 5

Le code Atbash était utilisé par les hébreux. Il consistait à inverser les lettres de l'alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Mot « Cryptogramme » crypté avec le code Atbash

Cryptogramme → Xibkgljitiznnv

Le chiffre Albam décale les lettres de l'alphabet de 13 positions sur la droite.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

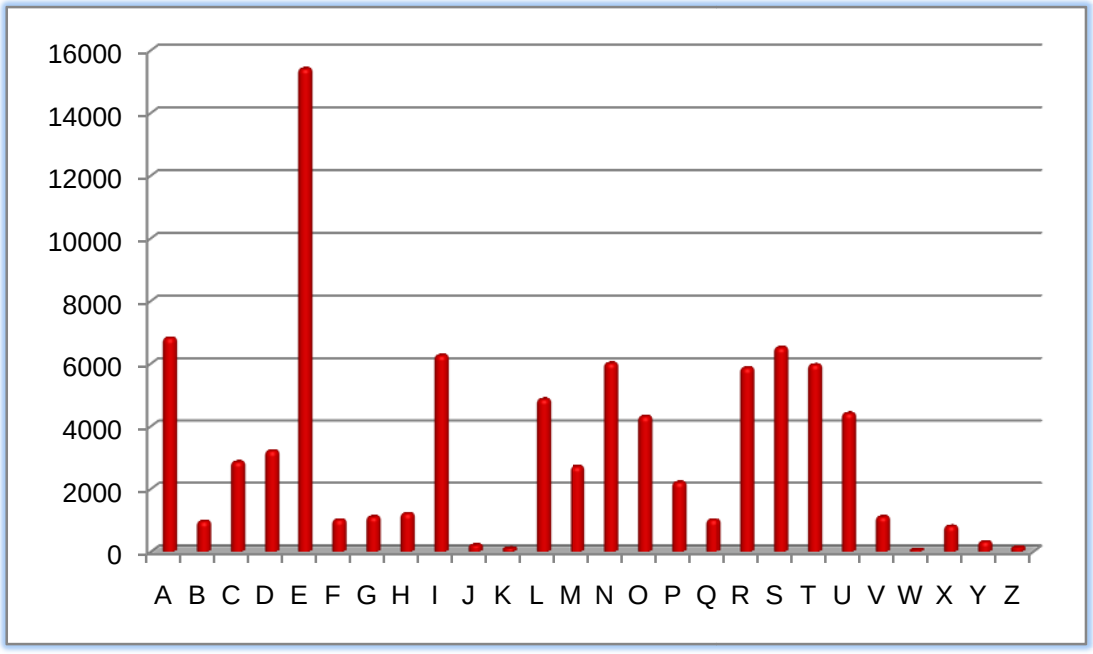
Mot « Cryptogramme » crypté avec le chiffre Albam :

Cryptogramme → Pelcgbtenzzr

Néanmoins la méthode de substitution comporte certaines faiblesses. Même si les 26 lettres de notre alphabet nous permettent un grand nombre de possibilités : 26 ! (403'291'461'126'605'635'584'000'000 possibilités), la fréquence de leurs apparitions facilite la déduction du mot caché.

Figure 43

Fréquence moyenne des lettres dans l'alphabet



Source : http://www.bibmath.net/crypto/substi/images/statlettre.gif

4.4.2. Fonction de Hachage

Le hachage permet d'obtenir un condensé du texte. Si le message est modifié avant son arrivée, le digest (message haché) ne correspondra plus au texte. Le texte haché ne permet pas de retrouver le message, seulement l'inverse est possible.

Un des plus connu est le MD5 (**M**essage **D**igest **5**). Il est obtenu par un calcul mathématique.

Mot « Cryptogramme » crypté en MD5 :

Cryptogramme → b94209bccb4feebfc977655a155d95a9

4.4.3. OTP

Mot de passe à usage unique (**O**ne **T**ime **P**asseword). Contrairement à la façon plus classique de s'identifier, c'est-à-dire un identifiant et un mot de passe, l'OTP n'est valide que pour une session et ce n'est pas l'utilisateur qui le choisit; il est généré préalablement par un calcul.

Figure 44
Système d'identification par OTP

Source : http://www.nis-infor.com/prod_fiche.php?from=prod&id_prod=120

Avantage :

- Le mot de passe n'est plus aussi simple que celui créé par l'utilisateur.
- Il n'est utilisé qu'une seule fois alors ne sera pas cracké.
- Il peut être envoyé en clair sur Internet car si un sniffer[31] l'intercepte, le mot de passe sera déjà obsolète.

Source : http://www.securiteinfo.com/cryptographie/otp.shtml

31 Permet d'écouter et d'intercepter les données envoyées sur Internet

4.4.4. Chiffrement synchrone

Les algorithmes de cryptage et de décryptage utilisent la même clef.

4.4.5. Chiffrement asynchrone

Le cryptage et le décryptage se font avec des clefs différentes.

4.4.6. Cryptographie symétrique – à clef privée

Chacun doit avoir la clef privée qui ouvrira le message mais pour cela il aura fallu au préalable procéder à un échange de clefs ce qui rend l'opération moins sûre. Cette méthode est très ancienne : à l'époque, les Américains transmettaient le message du lieu de rendez-vous aux alliés par le fameux téléphone rouge puis une valise était acheminée vers cet endroit et c'est là que l'information était échangée, comme ici la clef que l'on échange.

4.4.6.1. AES

L'AES (**A**dvanced **E**ncryption **S**tandard) est un standard de cryptage symétrique et par blocs (de 128 bits).

Avantage :

- Calculs assez simples, donc transmission des données plus rapides.
- Pas besoin de beaucoup de ressources mémoires.
- Il peut être sous forme de logiciel ou matériel.

Par ces caractéristiques, on voit qu'il convient tout particulièrement aux systèmes embarqués tels que les téléphones mobiles.

Source : http://www.securiteinfo.com/cryptographie/aes.shtml

4.4.6.2. SSL

Le SSL (**S**ecure **S**ocket **L**ayer) est un protocole de sécurité qui utilise l'algorithme de chiffrement symétrique. Il assure trois objectifs de la sécurité informatique. La **confidentialité**, l'**intégrité** et l'**authentification**. Un avantage qu'il propose est sa transparence par rapport au protocole TCP[32]. Le SSL est beaucoup utilisé dans le monde entier.

Les faiblesses du SSL

Les clefs plus basses que 128 bits sont vulnérables aux attaques par force brute[33]. La vérification de certificats n'est pas très sévère avec le SSL c'est pourquoi la sécurité est assez faible. Le SSL est aussi susceptible aux attaques « man-in-the-middle ». Cette attaque consiste à avoir une tierce personne (un hacker) qui intercepte le message entre deux utilisateurs; elle peut le lire, le modifier ou insérer des informations sans que le destinataire ni l'expéditeur ne s'en rende compte.

Source : http://www.securiteinfo.com/cryptographie/ssl.shtml

4.4.7. Cryptographie asymétrique – à clef publique

La cryptographie asymétrique utilise une clef publique. Elle est diffusée et permet de coder le message. Une clef privée ou secrète permet de décoder le message. L'expéditeur peut coder le message que seul le destinataire pourra décoder.

4.4.7.1. PKI

La PKI (**P**ublique **K**ey **I**nfrastructure) permet la gestion de clefs publiques par des certificats numériques. C'est un ensemble de gestion de sécurité. L'infrastructure PKI propose plusieurs services : la publication, le renouvellement et la révocation de certificats. Elle publie la **L**iste des **C**ertificats **R**évoqués (CRL) et s'occupe aussi de l'enregistrement, l'**authentification** et l'**identification** des utilisateurs.

32 Protocole de control de transmission

33 Méthode qui consiste à tester toutes les possibilités pour trouver un mot de passe ou une clef

Plusieurs éléments composent cette infrastructure :

- **Autorité de Certification** (CA) qui signe les certificats (CSR) et les listes de révocation (CRL).
- **Autorité d'Enregistrement** (RA) qui fait l'intermédiaire, l'interface entre le demandeur et l'autorité de certification.
- **Autorité de Dépôt** (Repository) qui publie les certificats et les liste de révocation (CRL), elle s'occupe donc du stockage.

4.4.7.2. RSA

Une des méthodes les plus connues de chiffrement à clef publique est le RSA qui a été inventé en 1977 par Ron **R**ivest, Adi **S**hamir et Len **A**dleman. Il est utilisé dans de nombreux sites web ainsi que pour les cartes bancaires françaises. La clef publique est disponible pour toute personne voulant chiffrer des données. La clef privée est pour la personne ayant créé la paire de clefs (voir Figure 45).

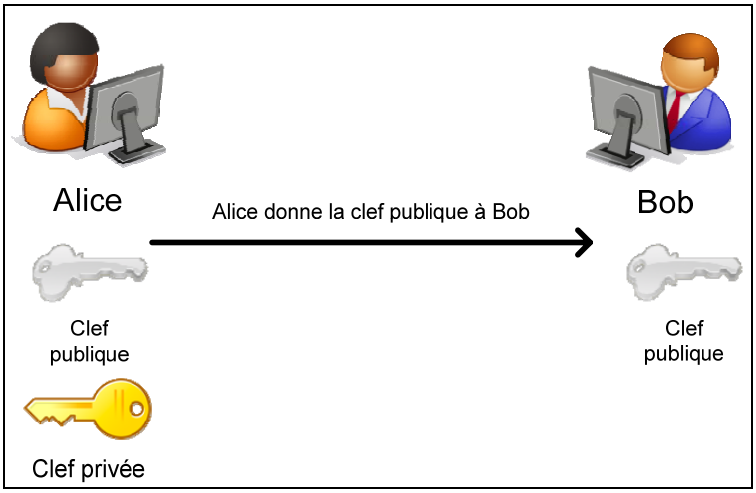
Source : http://www.bibmath.net/crypto/moderne/rsa.php3

Le RSA est-il sûr ?

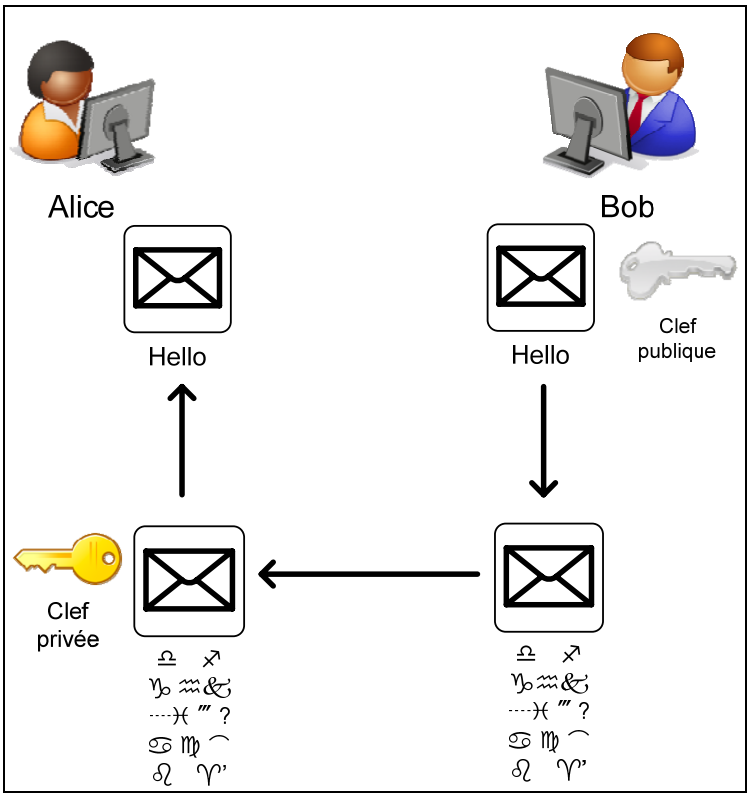
Le RSA est utilisé depuis plus de 25 ans et n'a toujours pas réussi à être cracké car pour pouvoir le faire il faut factoriser le nombre « n » ce qui prend énormément de temps. Afin de garantir une plus grande sécurité, il faut choisir des clefs relativement grandes, au minimum de 1024 bits. Le plus grand nombre factorisé n'étant pas plus long que 663 bits, il reste encore une marge avant d'atteindre les 1024. Cependant une clef de 2048 bits ou davantage demeure la solution la plus sûre car il sera impossible de la décrypter… avant des décennies.

En France, ce n'est que depuis 2004 que l'on peut utiliser des clefs de la longueur désirée; auparavant la limite était de 128 bits. L'armée voulant avoir la possibilité de cracker les clefs, elle n'autorisait pas l'utilisation de plus grandes. Ceci est toujours le cas aux Etats-Unis; la Suisse, quant à elle, n'a jamais été soumise à ces restrictions.

Figure 45
Cryptographie asymétrique



Alice génère 2 clefs, une publique (grise) qu'elle va envoyer à Bob et une clef privée (jaune) qu'elle garde pour elle.



Bob va chiffrer le message avec la clef publique (grise) puis Alice déchiffre avec sa clef privée (jaune).

4.5. S/MIME

Le RSA a développé le protocole S/MIME (**S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions) qui sert à renforcer la sécurité du courrier électronique. Il permet d'envoyer des signatures numériques même depuis un système d'exploitation Windows à un système d'exploitation totalement différent tel que Unix. Pas besoin d'installer d'autres logiciels pour recevoir les e-mails. Il utilise le principe du chiffrement à clef publique.

S/MIME fournit aussi trois objectifs de la sécurité informatique : l'**intégrité**, l'**authentification** et la **non-répudiation** des données.

4.6. Single-Sign-On

L'authentification unique, en anglais **S**ingle-**S**ign-**O**n (SSO) permet à un utilisateur de s'identifier une seule fois pour accéder à plusieurs applications informatiques.

Avantage :

- Simplifie la tâche de l'utilisateur, pas besoin de s'authentifier plusieurs fois, il y a donc moins de chance de confondre les mots de passe.
- La gestion des mots de passe est plus simple à gérer. Le problème de la sécurité est souvent dû à l'être humain. Si l'on a beaucoup de mots de passe à gérer, on aura tendance à les écrire sur un bout de papier et ceci est l'une des nombreuses brèches que l'on peut trouver.

Inconvénient :

- L'annuaire est très sensible car il contient les identités de tous les utilisateurs.
- Si une personne trouve le mot de passe, il aura accès à toutes les applications.
- Les mots de passe doivent être souvent changés donc il y a un risque que les gens les notent ou ne s'en souviennent plus.

Trois approches :

Approche centralisée

- Une base de données ou un annuaire pour tous les utilisateurs.

Approche fédérative

- Chaque service gère les données de l'utilisateur qui peut donc posséder plusieurs comptes. Les informations sont cependant partagées avec les services partenaires.

Approche coopérative

- Chaque utilisateur dépend d'un partenaire et quand il cherche une information, il est authentifié par celui dont il dépend. Cette approche ressemble à la fédérative mais chaque partenaire a sa propre politique de sécurité.

4.7. La signature numérique

La signature numérique est un procédé qui permet d'assurer que l'émetteur du message est bien le bon et de vérifier son **intégrité**. Plusieurs conditions doivent être réunies dans ce but : l'identité de la personne qui a signé le document doit être retrouvable et véridique et ne peut pas être niée. Cette signature ne doit pas être falsifiable, modifiable ni réutilisable.

.

4.7.1. Norme X.509

La norme X.509 est un standard de l'union internationale des télécommunications pour les infrastructures à clefs publiques sous forme de document électronique signé avec une empreinte digitale. Elle prouve l'identité de l'utilisateur auprès de l'autorité de certification et montre les droits de cet utilisateur ainsi que la validité de sa clef.

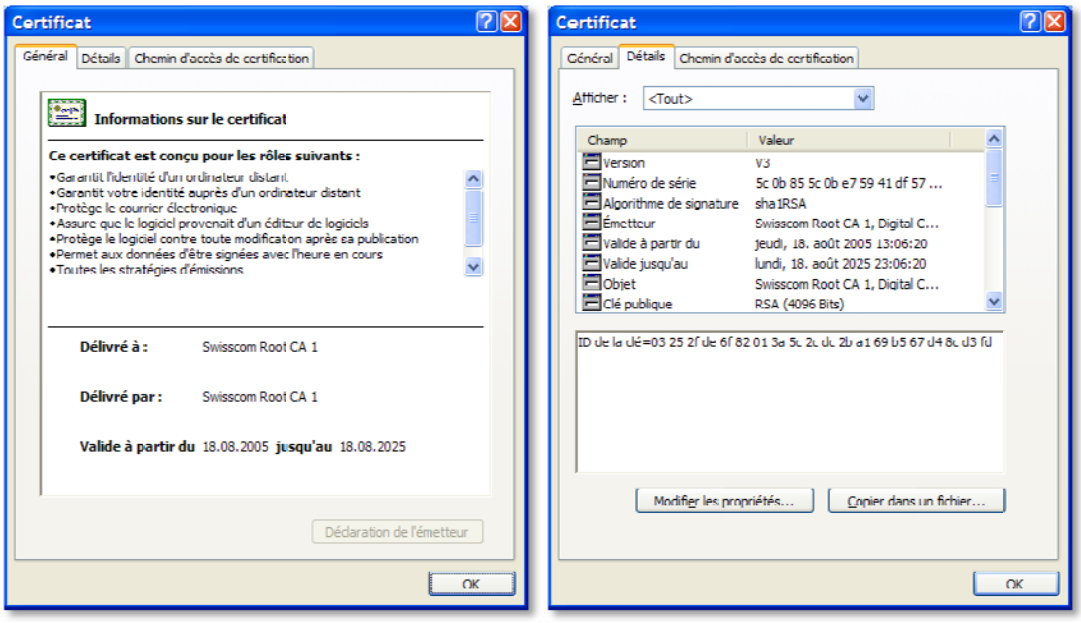
Fonctionnement :

Une autorité de certification donne un certificat qui lie une clef publique à un nom distinctif (e-mail ou nom de domaine).

Figure 46
Certificat de norme X.509

Source : http://www.formation.ssi.gouv.fr/stages/documentation/architecture_securisee/cours_crypto_certif.html

Figure 47
Certificat Swisscom[34]



34 Compagnie suisse de téléphonie

4.7.2. Textes de loi suisse sur la signature électronique

« *Disposition légale*

Art. 2 Définitions

1. *Au sens de la présente loi, on entend par :*

   a. *signature électronique : **données électroniques** jointes ou liées logiquement à d'autres données électroniques et **qui servent à vérifier leur authenticité;***

   b. signature électronique avancée : signature électronique qui satisfait aux exigences suivantes :

   c. être liée uniquement au titulaire,

   d. permettre d'identifier le titulaire,

   e. être créée par des moyens que le titulaire peut garder sous son contrôle exclusif,

   *f. être liée aux données auxquelles elle se rapporte de telle sorte que **toute modification ultérieure des données soit détectable;***

   g. signature électronique qualifiée : signature électronique avancée fondée sur un dispositif sécurisé de création de signature au sens de l'art. 6, al. 1 et 2, et sur un certificat qualifié valable au moment de sa création;

2. *clé de signature : données uniques telles que des codes ou des clés cryptographiques privées que le titulaire utilise pour composer une signature électronique;*

   a. clé de vérification de signature : données telles que des codes ou des clés cryptographiques publiques utilisées pour vérifier une signature électronique;

   b. certificat qualifié : certificat numérique qui remplit les conditions de l'art. 7;

   c. fournisseur de services de certification (fournisseur) : organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques;

   d. organisme de reconnaissance : organisme qui, selon les règles de l'accréditation, est habilité à reconnaître et à surveiller les fournisseurs. »

Source : http://www.admin.ch/ch/f/rs/9/943.03.fr.pdf (p.1 et 2)

« Section 3 Elaboration et utilisation de clés de signature et de vérification de signature

Art. 6

1. *Le Conseil fédéral règle l'élaboration des clés de signature et de vérification de signature pouvant faire l'objet de certificats qualifiés au sens de la présente loi. Ce faisant,* ***il veille à assurer un degré de sécurité élevé, conforme à l'évolution de la technique.***

2. *Les dispositifs de création de signature doivent au moins :*

   a. *garantir que la clé de signature utilisée pour l'élaboration de la signature ne puisse pratiquement se rencontrer qu'une seule fois et que sa* ***confidentialité soit suffisamment garantie;***

   b. *assurer avec une marge de sécurité suffisante que la clé de signature utilisée pour la création de* ***la signature ne puisse être trouvée par déduction*** *et que* ***la signature soit protégée contre toute falsification*** *par les moyens techniques disponibles;*

   c. *garantir que la clé de signature utilisée pour la création de* ***la signature puisse être protégée de manière fiable*** *par le titulaire légitime contre toute utilisation abusive.*

3. *Lors de la mise en place du processus de vérification de la signature, il convient de veiller à ce que les exigences suivantes soient remplies avec une marge de sécurité suffisante :*

   a. *les données utilisées pour vérifier* ***la signature correspondent aux données affichées à l'intention du vérificateur;***

   b. *la signature est vérifiée de manière sûre et le résultat de cette vérification est correctement affiché;*

   c. *le vérificateur peut, si nécessaire, déterminer de manière sûre le contenu des données signées;*

   d. *l'authenticité et la validité du certificat requis lors de la vérification de la signature sont vérifiées de manière sûre et le résultat de cette vérification est correctement affiché;*

   e. *l'identité du titulaire de la clé de signature est correctement affichée;*

   f. *l'utilisation d'un pseudonyme est clairement indiquée;*

   g. *tout changement ayant une influence sur la sécurité peut être détecté »*

Source : http://www.admin.ch/ch/f/rs/9/943.03.fr.pdf (p.4)

« Art. 14 Protection des données

1. *Les fournisseurs reconnus et les bureaux d'enregistrement qu'ils ont mandatés ne peuvent traiter que les données personnelles nécessaires à l'accomplissement de leurs tâches.* ***Tout commerce de ces données est interdit.***

2. *Au surplus, la législation sur la protection des données est applicable. »*

Source : http://www.admin.ch/ch/f/rs/9/943.03.fr.pdf (p.7)

« Ordonnance sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE)

Du 3 décembre 2004 (Etat le 21 décembre 2004)

Art. 3 Clés de signature et de vérification de signature

1. *Pour pouvoir faire l'objet de certificats qualifiés,* ***les clés de signature et de vérification de signature doivent avoir une longueur suffisante et mettre en œuvre un algorithme reconnu*** *pour être à même de résister à des attaques cryptographiques durant la période de validité du certificat qualifié.*

2. *L'office règle les détails dans les prescriptions techniques et administratives et fixe les exigences applicables aux dispositifs de création de signature. Il peut également fixer des exigences pour le processus de vérification de la signature. »*

Source : http://www.admin.ch/ch/f/rs/9/943.032.fr.pdf (p.1)

Mise en perspective

Si nous résumons les chapitres précédents, nous nous apercevons que certaines solutions sont plus sûres que d'autres ou plus prometteuses. Vous pouvez déjà commencer à faire votre propre dossier médical avec Google Health ou attendre celui de la stratégie eHealth mais pour cela il faudra compter encore quelques années. Les moyens mis en œuvre sont disponibles, les infrastructures de communication, de certificats et les lois correspondent aux attentes que l'on peut avoir. Les HUG et leur principe de vitre brisée sont un bon exemple de procédure interne de sécurité; si des actions comme celles-ci sont définies pour tous les projets, nous sommes sur la bonne voie et la sécurité ne devrait plus être une préoccupation. On trouvera ci-dessous un tableau récapitulatif des différents projets et systèmes déjà en exploitation.

Tableau 5

Récapitulatif des projets et systèmes en exploitation

	Fonction	Sécurité et normes utilisées	Niveau de sécurité
HIN	Plateforme de transaction sécurisée	Joue le rôle d'autorité de certification	Elevé
ASAS	Système de sécurité HIN	Cryptage end-to-end Norme X.509 OCV PKI RSA S/MIME Signature digitale SSL SSO	Elevé
HIN MailGateway	Passerelle d'envoi de courrier électronique	Cryptage end-to-end Norme X.509 RSA S/MIME Signature numérique	Elevé Authenticité Intégrité
OVAN	Réseau VPN	Firewall SSO	Elevé
H-Net	Plateforme de transaction sécurisée	SSL	Elevé

Covercard®	Carte d'assuré	➔ Clef univoque sur la carte - encodée sur la bande magnétique ➔ Norme X.509 ➔ SSL3	Moyen - Bas
Stratégie eHealth : ➔ *Dossier électronique du patient*	Dossier médical informatisé accessible via Internet	➔ Base de données centralisée ➔ Signature électronique	Elevé
Stratégie eHealth : ➔ *Service en ligne*	Portail de santé		
Stratégie eHealth : ➔ *Carte d'assuré*	Carte avec données médicales facultatives	➔ Code PIN ➔ Signature électronique en option.	Moyen – Elevé
Dossier Patient Intégré (DPI)	Dossier médical informatisé des patients aux HUG	➔ Carte à puce (SSO) ➔ Principe de vitre brisée	Elevé
Carte Professionnelle Santé (CPS)	Identifie le détenteur de la carte et ses droits	➔ Signature numérique	Elevé
Projet e-Toile	Entité qui permet l'accès aux données médicales de divers instituts de soins	➔ Accès traçables ➔ Cryptage ➔ Décentralisé	Elevé
VeriChip	Puce électronique sous-cutanée	➔ RFID	Moyen
Carte Vitale	Carte d'assuré pour les citoyens français	➔ Carte à puce	Bas
Google Health	PHR – Dossier personnel de santé	➔ SSO	Moyen

Conclusion

Par principe, nous sommes tous attachés à la confidentialité de nos données pour autant que des règles sûres soient mises en place.

En résumé, de qui voulons-nous nous protéger sachant que les assurances ont accès à toutes nos données médicales ? Faut-il craindre quelque chose ou quelqu'un étant donné que le système actuel est déjà transparent ? La technologie informatique est-elle plus dangereuse que toute autre forme de transaction ?

Aujourd'hui il semble que la mise en place d'un système de cybersanté est devenue incontournable; bien sûr certains y verront toujours des inconvénients mais d'ores et déjà, pour la majorité des personnes, les avantages paraissent évidents.

Le fait que certains se méfient de la question de la sécurité des données, à juste titre ou non, pourrait les empêcher de se confier à leurs médecins par peur que des informations les concernant circulent et soient interceptées. Cette crainte de la transparence pourrait affecter les diagnostics et les traitements.

Un cas concret récent vient agrémenter mon mémoire et confirmer mon opinion sur la cybersanté. Un proche de ma famille a dernièrement consulté plusieurs médecins pour des problèmes respiratoires. Son médecin traitant l'a dirigé vers différents spécialistes, un pneumologue, un cardiologue; chacun de son côté a fait de nombreux examens et analyses, sans grands résultats. Après plusieurs malaises assez inquiétants, il a recontacté le pneumologue pour un rendez-vous urgent; la secrétaire a répondu qu'il rentrait de vacances et n'avait pas le temps de le recevoir. Le lendemain il a refait un malaise et c'est en hélicoptère qu'il est arrivé aux urgences des HUG aux soins intensifs.

Dans la pratique, aux HUG les différents spécialistes investiguent pour trouver les causes et les données médicales sont instantanément coordonnées. Faut-il attendre d'avoir une attaque pour que l'on prenne notre santé au sérieux ? Il est prouvé que des informations immédiatement disponibles permettent un diagnostic plus rapide et constituent un gain de temps précieux surtout en cas de problème grave. Voilà pourquoi le dossier du patient que la stratégie eHealth veut mettre en place est très important, pour que des accidents de ce genre ne se reproduisent plus et que les médecins coopèrent ensemble.

Pour terminer, mon opinion sur le sujet est la suivante : je suis favorable à la mise en place d'une stratégie de cybersanté et la sécurité des données ne m'inquiète pas, pour autant qu'elle soit bien gérée…la vigilance est donc de mise.

Index

A

ACS 27, 28, 90
ADSL 24, 90
AES 73, 90
Antivirus 29, 30
ASAS 18, 24, 26, 27, 28, 29, 83, 90
Authenticité 28, 80, 81, 83
Authentification 18, 24, 36, 37, 65, 74, 77, 91

C

CA 75, 90
CDA 53, 90
CERT 68, 90
CLUSIF 68, 90, 93
CLUSIS 68, 90
CO 14, 90
Confidentialité 2, 40, 41, 54, 60, 61, 63, 64, 74, 81, 85, 92
Cookies 60, 90
Covercard® 31, 32, 33, 84
CPS 13, 84, 91
CPS - HPC 49, 91
Cracké 72, 75
CRL 74, 75, 91
Cryptographie
- Chiffrement 4, 29, 64, 73, 74, 75, 77, 90
- Chiffrer 75, 76
- Cryptage 4, 24, 26, 29, 43, 73, 83, 84, 91
- Crypter 20, 28, 42, 70, 71, 72
- Cryptogramme 70, 71, 72
- Cryptographie 70, 73, 74, 76, 80, 82, 94
- Cryptologie 70
- Déchiffrer 76
- Décryptage 73
- Décrypter 28

CSCQ 54
CSR 75, 91
CUMUL 53, 54
Cybersanté 1, 4, 5, 12, 33, 36, 39, 85, 91

D

DBA 17, 91

DICOM 53, 91

Disponibilité 64, 92

DMZ 28, 91

DPI 44, 54, 55, 84, 91, 108

E

e-banking 35, 91

eDAGate 21

eHealth 33, 34, 35, 37, 39, 83, 84, 85, 91

end-to-end 24, 26, 83, 91

e-Toile 50, 51, 84, 94

F

Firewall 30, 83, 91

FSASD 3, 55, 91

G

Geek 65, 92

Google 59, 60, 61, 62, 63

Google Health 59, 61, 62, 63, 83, 84

GPS 56, 92

H

Hacker 35, 65, 74, 92

HEG 1, 2, 92

HIN 18, 24, 25, 26, 27, 28, 29, 30, 33, 83, 90, 92

HIPAA 61, 62, 92

HL7 ..... 52, 53, 90, 92

H-Net 25, 30, 33, 83, 92

HON 40, 92

HONcode 40, 41, 42, 92

HUG 3, 5, 17, 26, 44, 45, 53, 54, 55, 83, 84, 85, 91, 92, 95

I

Input Gate 21

Intégrité 28, 64, 74, 77, 78, 83, 92

L

LAMal 15, 16, 93

Log 47, 93

LOINC 53, 54, 93

LPD 18, 93

M

man-in-the-middle 74, 93
MD5 ..... 72, 93
MEHARI 68, 93

N

NewIndex 24, 93, 95
Non-répudiation 64, 77
Norme X.509 ..... 26, 28, 32, 78, 79, 83, 84, 93

O

OCV 26, 28, 83, 93
Ofac 25, 31, 93, 94
OFSP 93
OMS 38, 40, 93
OSI 52, 94
OTP 72, 94
OVAN 25, 26, 33, 83, 94

P

PHR 59, 84, 94
PIN 48, 84, 94
PKI 26, 28, 74, 83, 94
Pocket PC 55
PostFinance 30, 31
Privacy International 60
Publifocus 35, 44, 94

R

RA 75, 94
RFID 56, 84, 94
RSA 26, 28, 75, 77, 83, 94

S

S/MIME 24, 26, 28, 77, 83, 94
Serment d'Hippocrate 15
Signature 78, 80, 81, 82, 91
  Signature électronique 36, 37, 80, 82, 84
  Signature numérique 28, 34, 77, 78, 83, 84
  Signatures digitales 26, 83
SIM 17, 95
Single-Sign-On 77

SSO 26, 27, 77, 83, 84, 95
SSL 26, 28, 32, 74, 83, 84, 95

T

TARMED 15, 93, 95, 102
TA-SWISS 35, 44, 94, 95
TCP 74, 95
TIC 33, 91, 95
Token 22, 23, 95
TrustCenter 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 95
TrustX 20, 21, 22, 24, 95

U

UNIGE 5, 95
Unix 77, 95

V

VeriChip 56, 57, 84
VPN 25, 33, 83, 95

W

Wifi 55, 95

X

XML 19, 53, 90, 96

Glossaire

ACS ***A**ccess **C**ontrol **S**ervice* : Liste de contrôle des autorisations d'accès établie par l'hôpital et géré par le centre de calcul de HIN.

ADSL ***A**symmetric **D**igital **S**ubscriber **L**ine* : Raccordement numérique qui permet de s'abonner à une ligne téléphonique et de surfer sur Internet à haut débit.

AES ***A**dvanced **E**ncryption **S**tandard* : Technique de chiffrement à clef symétrique de longueur minimum de 128 bits.

ASAS ***A**rpage **S**ecurity and **A**ccess **S**ervices* : Système de sécurité utilisé par la plateforme HIN.

CA ***C**ertification **A**uthority* : En français : Autorité de Certification. C'est lui qui signe les certificats et les listes de révocations.

CDA ***C**linical **D**ocument **A**rchitecture* : Document destiné à l'échange de type XML ou HL7 et pouvant être lu avec un navigateur Internet.

CERT ***C**omputer **E**mergency **R**esponse **T**eam* : Organisme qui gère les incidents informatiques.

CLUSIF ***CLU**b de la **S**écurité de l'**I**nformation **F**rançais* : Club qui accueille des entreprises ou des collectivités pour agir sur la sécurité des systèmes d'informations.

CLUSIS ***CLU**b de la **S**écurité de l'**I**nformation **S**uisse* : Club suisse rattaché au CLUSIF.

CO ***C**ode des **O**bligations* : Règle la forme des contrats entre deux parties.

Cookies Fichiers textes qui recensent des informations sur la navigation de l'internaute à des fins de marketing ou pour simplifier les prochaines visites d'un site en gardant par exemple la langue choisie.

CPS - HPC ***C**arte **P**rofessionnelle de **S**anté*, ***H**ealth **P**rofessional **C**ard*, en anglais : Permet de s'identifier en tant que médecin. Elle garantie une authentification sans équivoque.

CPS ***C**ode **P**énal **S**uisse* **:** Code pour punir des personnes morales ou physiques.

CRL ***C**ertificate **R**evocation **L**ist* : Liste de révocation des certificats volés ou perdus.

CSR ***C**ertificate **S**igning **R**equest* : Demande de signature de certificat.

Cybersanté Service de santé électronique.

DBA ***D**ata **B**ase **A**dministrator* : L'administrateur de bases de données est celui qui gère et donne les droits et l'accès aux données aux utilisateurs.

DICOM ***D**igital **I**maging and **CO**mmunications in **M**edicine* : Standard de communication en imagerie médicale.

DMZ ***D**e**M**ilitarized **Z**one* : Zone démilitarisée qui se trouve entre le réseau interne et le réseau externe (Internet). Il est protégé par un firewall (coupe-feu).

DPI ***D**ossier **P**atient **I**ntégré* : Dossier médical informatisé aux HUG.

E2E ***e**nd-**to**-**e**nd* **:** Cryptage de "bout en bout", cela signifie que la connexion est cryptée entre votre ordinateur et le serveur.

e-banking Principe de traitement des opérations bancaires par Internet.

eHealth ***e**lectronic **Health** (cybersanté)* : désigne «l'utilisation des technologies de l'information et de la communication (TIC) pour l'organisation, le soutien et la mise en réseau de tous les processus et partenaires impliqués dans le système de santé.» (Définition de l'Office fédéral de la santé publique OFSP).

FSASD ***F**ondation des **S**ervices d'**A**ide et de **S**oins à **D**omicile* : Centre d'action sociale et de santé dans le canton de Genève.

Geek **T**erme utilisé pour décrire une personne passionnée voire même obsédée par le milieu informatique, la programmation, les jeux, les technologies…

GPS ***G**lobal **P**ositioning **S**ystem* : Système de géolocalisation par satellite. Il a été développé par l'armée américaine et est mis à la disposition des gens pour un guidage routier ou aérien au moyen d'un boîtier et d'un logiciel de cartographie.

Hacker Pirate informatique.

HEG ***H**aute **E**cole de **G**estion* : Etablissement de formation supérieure reliée aux **H**autes **E**coles **S**pécialisées de **S**uisse **O**ccidentale (HES-SO). Elle regroupe trois filières : Economie d'entreprise, Information documentaire et Informatique de gestion.

HIN ***H**ealth **I**nfo **N**et* : Plateforme Extranet sécurisée dans le domaine de la santé.

HIPAA ***H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct* : Loi étasunienne sur la protection des données médicales et sur la vie privée du patient. Les transactions électroniques et l'encodage des données ainsi que leurs intégrités, disponibilités et confidentialités.

HL7 ***H**ealth **L**evel **7*** : Standard d'échange de fichiers médicaux.

H-Net Plateforme de transactions de données médicales.

HON ***H**ealth **O**n the **N**et* : HON est une organisation non gouvernementale (ONG) qui a été créée pour accroître la fiabilité et la qualité de l'information médicale sur Internet.

HONcode ***Code** de déontologie de **H**ealth **O**n the **N**et* : Est le plus utilisé et le plus ancien. Plus de 5'000 sites web certifiés l'utilisent dans 72 pays.

HUG ***H**ôpitaux **U**niversitaires de **G**enève* : Hôpital universitaire public basé à Genève.

IP ***I**nternet **P**rotocol* : Adresse qui identifie un ordinateur ou autre composant (imprimante, routeur) connecté à Internet. Elle se

présente sous cette forme : 192.168.1.55 Les chiffres sont compris entre 0 et 255 et sont séparés par des points.

LAMal ***L**oi sur l'**A**ssurance **Mal**adie* : Réglemente l'assurance maladie obligatoire en Suisse.

Log Est un fichier qui garde l'historique des manipulations faites sur un ordinateur. C'est comme un journal de bord où l'on peut retrouver la trace de qui à fait quoi, quand et où.

LOINC ***L**ogical **O**bservations, **I**dentifiers, **N**ames, and **C**odes* : Répertoire référentiel américain des analyses cliniques.

LPD ***L**oi sur la **P**rotection des **D**onnées* : Protéger la personnalité et les droits fondamentaux en donnant aux personnes la possibilité de savoir si des tiers disposent d'informations privées à leur sujet.

MD5 ***M**essage **D**igest **5*** : Algorithme de hachage.

MEHARI ***ME**thode **H**armonisée d'**A**nalyse de **R**isques* : Méthode de gestion des risques, créée par le CLUSIF.

MITM ***M**an **I**n **T**he **M**iddle* : Une machine se fait passer pour une autre et intercepte le trafic sur le réseau.

NewIndex Soutient les organisations du corps médical à mettre en place le nouveau tarif médical (TARMED). NewIndex doit développer de nouvelles solutions.

Norme X.509 Document électronique signé avec une empreinte digitale.

OCV ***O**nline **C**ertificate **V**alidation* : Identification des partenaires en ligne.

Ofac Coopérative professionnelle des pharmaciens suisses.

OFSP ***O**ffice **F**édéral de la **S**anté **P**ublique* : Fait parti du Département fédéral de l'intérieur et promeut la santé des citoyens suisses.

OMS ***O**rganisation **M**ondiale de la **S**anté* : Basée à Genève, elle est chargée de se préoccuper de la santé mondiale.

OSI ***O**pen **S**ystems **I**nterconnection* : Modèle de communications entre ordinateurs qui décrit les fonctionnalités essentielles à la communication et à l'organisation de ces fonctions.

OTP ***O**ne **T**ime **P**asseword* : Mot de passe à utilisation unique, par exemple avec une calculatrice qui génère aléatoirement un nouveau code.

OVAN ***O**fac **V**alue **A**dded **N**etwork* : Réseau virtuel sécurité destiné au secteur médical.

PHR ***P**ersonal **H**ealth **R**ecord* : Dossier médical personnel.

PIN ***P**ersonal **I**dentification **N**umber* : NIP en français pour **N**uméro d'**I**dentification **P**ersonnel, il s'agit d'un code confidentiel constitué de chiffres afin d'authentifier le détenteur d'une carte à puce.

PKI ***P**ublic **K**ey **I**nfrastructure* : Ensemble de gestion de sécurité qui permet la distribution de clefs publiques par des certificats.

Publifocus Méthode participative développée par TA-SWISS qui sert à intégrer des citoyens à des prises de décisions politiques dans le domaine des technologies.

RA ***R**ecord **A**uthority* : En français : autorité d'enregistrement qui fait l'intermédiaire, l'interface entre le demandeur et l'autorité de certification pour l'obtention d'un certificat numérique.

RCIM ***R**éseau **C**ommunautaire d'**I**nformatique **M**édicale* : Permet aux professionnels de la santé de se brancher sur un réseau informatique. Le projet e-Toile fait parti d'un RCIM.

RFID ***R**adio **F**requency **ID**entification* : L'identification par onde radio est une méthode pour récupérer et récolter des données à distance.

RSA ***R**on **R**ivest, Adi **S**hamir, Len **A**dleman* : Algorithme de cryptographie à clef publique.

S/MIME ***S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions* : Protocole qui sert à renforcer la sécurité du courrier électronique.

SIM ***S**ervice d'**I**nformatique **M**édicale* : Rattaché à la Faculté de Médecine des HUG, le SIM travaille aussi à faire avancer la recherche dans le domaine de l'informatique médicale et enseigne cette discipline, aussi bien aux étudiants en médecine que dans le cadre de formations post-graduées.

SSL ***S**ecure **S**ocket **L**ayer* : Norme de sécurité de transfert de données.

SSO ***S**ingle-**S**ign-**O**n* : Permet de s'identifier qu'une seule fois pour plusieurs applications.

TARMED ***Tar**if **Méd**ical* : Système de facturation électronique utilisé en Suisse.

TA-SWISS Centre d'évaluation des choix technologiques suisses.

TC ***T**rust**C**enter* : Centres fiduciaires qui sont des points de recueil pour les données des facturations médicales Le concept des TrustCenter a été créé par NewIndex.

TCP ***T**ransmission **C**ontrol **P**rotocol* : Protocole de transfert de données surtout utilisé avec Internet.

TIC ***T**echnologies de l'**I**nformation et de la **C**ommunication* : Moyens utilisés dans le traitement et l'envoi de données notamment en informatique et dans les télécommunications.

Token Identificateur, dans ce cas, il s'agit d'un numéro unique inscrit sur le bulletin de versement qui correspond à un patient.

TrustX Interface logicielle entre l'entité médicale et le TrustCenter qui permet d'exporter et transmettre les facturations des patients.

UNIGE ***UNI**versité de **GE**nève*.

UNIX Système d'exploitation.

VPN ***V**irtual **P**rivate **N**etwork* : Réseau virtuel.

WIFI Technique de réseau sans fil.

XML *e**X**tensible **M**arkup **L**anguage* : Langage informatique de description de documents qui utilise des balises (marques) que l'on peut personnaliser et permet l'échange de données. Exemple de code XML pour les informations d'un patient (son nom, prénom, adresse) :

```
<?xml version="1.0"?>
<!DOCTYPE adresses>
<adresses>
 <patient id="1">
  <nom>Schauli</nom>
  <prenom>Eléonore</prenom>
  <rue>Ch. Du Claiset 17</rue>
  ...
 </ patient >
</adresses>
```

Bibliographie[35]

Documents référencés

- Agence de Presse Médicale. *La faille de la carte Vitale sera corrigée au premier semestre 2006. - Réseau Sésam-Vitale* [en ligne]. 13.12.2005. http://www.portailtelesante.org/article.php?sid=952

- BAKER, Wade H. HYLENDER, David C. VALENTINE, Andrew J. *2008 Data Breach Investigations Report* [en ligne]. 2008. http://www.verizonbusiness.com/resources/security/databreachreport.pdf

- BANCAL, Damien. *La nouvelle Carte Vitale 2 passe par FIME* [en ligne]. 12.11.2007. http://www.zataz.com/communique-presse/15647/La-nouvelle-Carte-Vitale-2-passe-par-FIME.html

- BAYART, Frédéric. *La cryptographie à clé publique – Le RSA* [en ligne]. http://www.bibmath.net/crypto/moderne/rsa.php3

- BOURQUARD, Karima. *Normalisation et Interopérabilité* [en ligne]. 19.07.2007. http://lertim.timone.univ-mrs.fr/Ecoles/infoSante/2007/supports_ppt/mercredi%2018%20juillet/Bourquart.pdf

- CFSSI. *Cours Cryptographie, Certificats IGC et OpenSSL* [en ligne]. http://www.formation.ssi.gouv.fr/stages/documentation/architecture_securisee/cours_crypto_certif.html

- CLUSIF. *Club de la Sécurité de l'Information Français* [en ligne]. http://www.clusif.asso.fr/

- COVERCARD. *Covercard® System* [en ligne]. Consulté et modifié le 10 novembre 2008. http://www.covercard.ch/FRN/

- CTÉSIAS. *Bienvenue chez Cetésias SA* [en ligne]. 2007. http://www.ctesias.ch/index.php?option=com_frontpage&Itemid=1

- CUMUL LOINC. *Version française* [en ligne]. Modifié le 1 décembre 2007. http://www.cumul.ch/

- ETAT DE GENEVE. *Rapport du Conseil d'Etat* [en ligne]. 2002. http://etat.geneve.ch/des/SilverpeasWebFileServer/iris_rapport.pdf?ComponentId=kmelia518&SourceFile=1125050473318.pdf&MimeType=application/pdf&Directory=Attachment/Images/&logicalName=iris_rapport.pdf

- FMH. *Codes diagnostics pour traitements ambulatoires* [en ligne]. http://www.fmh.ch/shared/data/pdf/annexe4b_diagnostic.pdf

- FMH. *Un risque pour la sécurité des patients et la protection des données – Une carte électronique de médecin pour une meilleure sécurité des patients.* In : Bulletin

35 Tous les ouvrages ont été consultés pendant la période du travail de Bachelor

des médecins suisses [en ligne]. 2007. http://www.saez.ch/pdf_f/2007/2007-38/2007-38-891.PDF

- GASSER, Jacques. *Le secret médical et quelques notions d'éthique* [en ligne]. 2006. http://www.unil.ch/webdav/site/fbm/shared/psyleg/secret_medical_et_ethique_9p.pdf

- GEISSBUHLER, Antoine. *Informatisation, qualité et efficience des processus de soins*. Présentation, 16.08.2008

- GEISSBUHLER, Antoine. *Un projet de réseau communautaire d'informatique médicale*. Présentation, 9.02.2006

- GEISSBUHLER, Antoine; GOBET, Gérard; UNGER, Pierre-François : Département de l'action sociale et de la santé. *e-toile - Un projet de réseau communautaire d'informatique médicale* [en ligne]. 2.11.2004. http://www.ta-swiss.ch/a/info_tele/041102_RE_geissbuhler_f.pdf

- Google Health. *Google Health Terms of Service* [en ligne]. 28.04.2008. http://www.google.com/intl/fr-CH/health/terms.html

- HERMANN, Vincent. *Sécurité en entreprise : l'erreur humaine est prépondérante Qui sera le maillon faible ?* [en ligne]. 06.10.2008. http://www.pcinpact.com/actu/news/46486-entreprises-securite-breches-protocoles.htm

- HIN Health Info Net SA. *Feuille d'information*. In : Abonnement [en ligne]. http://service.escapenet.ch/publisher/pictures/280/181083/Factsheet_HIN_Abo_f.pdf

- HIN Health Info Net SA. *Dispositions-cadres relatives à la transmission électronique de données* [en ligne]. 1.07.2000. http://www.hin.ch/f/pdf/rahmenbedingungen_f.pdf

- HIN Health Info Net SA. *Rapport annuel 2007* [en ligne]. http://www.hin.ch/f/pdf/gb_2007.pdf

- HIN Health Info Net. *Bienvenue sur Health Info Net* [en ligne]. http://hin.escapenet.ch/f/home.asp

- HIN Health Info Net. *HIN Covercard Service - et tout devient plus simple* [en ligne]. http://www.hin.ch/f/pdf/HIN_Covercard_Service_factsheet.pdf

- H-net. *Le réseau de santé suisse.* In : *Feuille d'information* [en ligne]. http://www.avintis.com/index.php?option=com_content&view=category&layout=blog&id=13&Itemid=15

- HON Health On the Net foundation. *Charte de "Health On the Net" (HONcode) destinée aux sites Web médicaux et de santé* [en ligne]. Modifié le 21 mai 2008. http://www.hon.ch/HONcode/index_f.html

- HPC NEWS. *HPC New, pour mieux vous informer. Toute l'actualité de HPC SYSTEM* [en ligne] Mars 2004. http://www.hpcsystem.ch/frn/HPCNewsFR_200403.pdf

- JACQUES, Arnaud. *La sécurité informatique – la sécurité de l'information. Les mots de passe à usage unique : One Time Password* [en ligne]. http://www.securiteinfo.com/cryptographie/otp.shtml

- JBK. *Gestion des dossiers médicaux par Google Health* [en ligne]. 29.05.2008. http://www.jbkempf.com/blog/post/2008/05/29/Gestion-des-dossiers-medicaux-par-Google-Health

- JisSoGoodToBe. *La sécurité informatique – la sécurité de l'information. L'AES : Advanced Encryption Standard* [en ligne]. http://www.securiteinfo.com/cryptographie/aes.shtml

- JisSoGoodToBe. *La sécurité informatique – la sécurité de l'information. SSL : Secure Socket Layer* [en ligne]. http://www.securiteinfo.com/cryptographie/ssl.shtml

- LAPOINTE, Michel. *Lois de l'informatique* [en ligne]. 26.01.1995. http://archimede.mat.ulaval.ca/guide/node109.html

- Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE 943.03) [en ligne]. http://www.admin.ch/ch/f/rs/9/943.03.fr.pdf

- LOVIS, Christian. *Dossier patient – Droits d'accès.* Support de cours. 18.01.2007

- LOVIS, Christian; SPAHNI, Stéphane. *Echanges sécurisés via HIN*. Support de cours. 9.02.2006.

- NEWINDEX. *Bienvenue chez NewIndex* [en ligne]. http://www.newindex.ch/f/home_intro.asp

- NIS – Smart Card Services. *Un service à la carte* [en ligne]. http://www.nis-infor.com/index.php

- No Microchip – No Chip. *Micro-puce sous-cutanée : la menace ultime pour l'humanité !* [en ligne]. Modifié le 29 septembre 2005. http://www.freewebs.com/nomicrochip/

- Office fédéral de la santé publique. *eHealth* [en ligne] http://www.bag.admin.ch/themen/krankenversicherung/04108/index.html?lang=fr

- Ordonnance du 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE 943.032) [en ligne]. http://www.admin.ch/ch/f/rs/9/943.032.fr.pdf

- PosteFinance LA POSTE. *H-Net* [en ligne]. 2008. http://www.postfinance.ch/pf/content/fr/seg/biz/product/eserv/filetransfer/hnet.html

- PRIVACY INTERNATIONAL. Consultation Report : Race to the Bottom ? [en ligne]. 2007. http://www.privacyinternational.org/issues/internet/interimrankings.pdf

- Projet de loi sur réseau communautaire d'informatique médicale du système de santé du canton de Genève (e-toile) (K 3 07) [en ligne]. http://www.geneve.ch/social/presse/doc/iris_projet_loi.pdf

- SANTE SUISSE. *La Façon de lire une facture TARMED* [en ligne]. http://www.santesuisse.ch/datasheets/files/200608091418300.pdf

- TRUSTX. *Médecins* [en ligne]. http://www.trustx.ch/f/home.asp

- TRUSTX. TrustX-Cabinet. *Description d'interface pour fournisseurs de logiciel médical [*en ligne]. 15.09.2005. http://www.trustx.ch/trustx-praxis/documents/Interface_TrustX-Cabinet_pour_editeurs_logiciels.pdf

- WIKIPEDIA. L'encyclopédie libre. *DICOM* [en ligne]. Modifié le 23 septembre 2008. http://fr.wikipedia.org/wiki/DICOM

- WIKIPEDIA. L'encyclopédie libre. *Serment d'Hippocrate* [en ligne]. Modifié le 14 octobre 2008. http://fr.wikipedia.org/wiki/Serment_d%27Hippocrate

Documents non référencés

- Confédération suisse. *Carte d'assuré* [en ligne]. http://www.bag.admin.ch/themen/krankenversicherung/04114/04126/index.html?lang=fr

- CyberEtat. *e-toile un réseau communautaire d'informatique médicale à Genève* [en ligne]. 26.03.2004. http://www.evanti.ch/NR/rdonlyres/9F4F5A4E-3947-486D-A9E4-D9880DCF5A4C/0/10_Tang_PresentationCyberEtat.pdf

- DATALOSS db open security foundation. *Incidents informatique* [en ligne]. http://datalossdb.org/

- DENZLER, Lukas; BRENNER, Susanne; BEN ZBIR, Nadia. *Nos données de santé en réseau. publifocus « eHealth et le dossier électronique du patient ».* In : Brochure d'information, [en ligne]. 2008. http://www.ta-swiss.ch/a/info_eHealth/web_bbl_gesundheit_f.pdf

- Dr. REY, Lucienne. *Pour un système de santé plus efficace. Rapport du processus de dialogue publifocus « eHealth et le dossier électronique du patient »* [en ligne]. 2008. http://www.ta-swiss.ch/a/info_eHealth/Bericht%20publifocus_ehealth_f.pdf

- DroitMedical. *Actualités, sources et services en droit médical suisse* [en ligne]. http://www.droitmedical.ch/

- GEISSBUHLER, Antoine. Département de l'action sociale et de la santé. *e-toile - Un projet de réseau communautaire d'informatique médicale* [en ligne]. 2.09.2005. http://etat.geneve.ch/des/SilverpeasWebFileServer/e-toile.pdf?ComponentId=kmelia518&SourceFile=1128066640016.pdf&MimeType=application/pdf&Directory=Attachment/Images/&logicalName=e-toile.pdf

- GEMALTO. *security to be free* [en ligne]. http://www.gemalto.com/index.html

- HOPITAUX UNIVERSITAIRES DE GENEVE, Département d'imagerie et des sciences de l'information médicale. *PDI – Présentation* [en ligne]. 22.02.2006. http://www.dim.hcuge.ch/dpi/01_DPI-Presentation_EN.htm

- OFCOM office fédéral de la communication. *Stratégie suisse en matière de cybersanté ("e-Health")* [en ligne]. http://www.bakom.admin.ch/themen/infosociety/01689/index.html?lang=fr

- OFSP, Office Fédéral de la Santé Publique. *Stratégie Cybersanté (eHealth) Suisse* [en ligne]. 27.06.2007.

- TARMED Suisse. *Bienvenus chez TARMED Suisse* [en ligne]. http://www.tarmedsuisse.ch/ueber_uns.html?&L=1

- WIKIPEDIA : L'encyclopédie libre. *Insécurité du système d'information* [en ligne]. http://fr.wikipedia.org/wiki/Ins%C3%A9curit%C3%A9_du_syst%C3%A8me_d'information

Annexe 1
Facture Tarmed

La façon de lire une facture TARMED:

Facture Release • 4.0 **M**

Document • 101 7333.0 24.02.2004 14:11:00.00 Page • 01

1 Auteur facture N° EAN • 7601000133333 Dr. med. Hans Muster 4055 Basel
N° RCC • L555555 Tel: 061 111 11 11 Fax: 061 111 11 11 E-mail:

2 Four. de prestations N° EAN • 7601000133333 Dr. med. Hans Muster 4055 Basel
N° RCC/No NIF • L555555 Tel. 061 111 11 11 Fax. 061 111 11 11 E-mail.

3 Patient
Nom • Muster
Prénom • Peter
Rue • Mustergasse 1
NPA • 4099
Localité • Basel
Date de naissance • 10.10.1942
Sexe • M
Date cas •
N° cas/décision •
N° AVS •
N° assuré • 100.100.000.
NP/Nom entreprise •
Canton • BS
Copie de facture • Non
Type de remb. • TP
Loi • LAA
Motif traitement • Accident
Traitement • 22.01.2004
Lieu fourn. prest. • Cabinet médical
No EAN •

4 Peter Muster
Mustergasse 1
4099 Basel

5 N° facture • 7333
Date facture/rappel • 24.02.2004

Mandataire N° EAN / N° RCC • 6
Diagnostic • N9 7
Liste EAN • 1/7601000128584
Commentaire HMO ÖKK

Date 8	Tarif 9	Code	Code réf.	Sé	Cô	Quantité	Pt PM/Prix 11	f PM	VPt PM 12	Pt PT 13	fPT	VPt PT 14	E	R	P	T	Montant 16
		Consultation, première période de 5 min (consultation de base)															
• 22.01.2004	001	00.0010				1 10	9.57		0.93	8.19		0.93	1	1	0	3	16.52
		+ Consultation, par période de 5 min en plus (supplément de consultation)															
• 22.01.2004	001	00.0020	00.0010			1	1	9.57	0.93	8.19		0.93	1	1	0	3	16.52
		+ Consultation, dernière période de 5 min (supplement de consultation)															
• 22.01.2004	001	00.0030	00.0010			1	1	4.78	0.93	4.10		0.93	1	1	0	3	8.26

1 Médecin qui établit la facture
2 Médecin qui fournit la prestation (le plus souvent identique à 1)
3 Données personnelles du patient
4 Adresse du destinataire de la facture
5 Numéro de la facture et date de la facture
6 Médecin, le cas échéant, qui a demandé le traitement
7 Code du diagnostic selon la liste des diagnostics
8 Dates des traitements
9 Numéro du tarif appliqué (par ex.: 001 = Tarmed, 316 = liste des analyses de laboratoire)
10 Quantités facturées par position de tarifs
11 Nombre de points de la prestation médicale. Par ex.: « Consultation, premières 5 minutes » , vaut 9,57 points
12 Valeur du point de la prestation médicale (actuellement la valeur est de CHF 0,93)
13 Nombre de points de la prestation technique
14 Valeur du point de la prestation technique
15 Code de la prestation prise en charge (0 = prestation prise en charge selon la LAMal, 1 = prestation non prise en charge)
16 Le montant en CHF des diverses positions du tarif se calcule de la manière suivante: (valeur du point de la prestation médicale x nombre de points de la prestation méd.) + (valeur du point de la prestation technique x nombre de points de la prestation technique).
17 Totaux partiels des divers domaines en CHF
18 Montant total de la facture en CHF

17 TARMED PM 22.25 (23.92) Physio 0.00 LiMA 0.00 Autres 0.00
TARMED PT 19.05 (20.48) Laboratoire 0.00 Médic. 0.00 Cantonal

18 • Montant total CHF 41.30 dont pr.obl. 41.30 Acompte 0.00 Montant dû 41.30

01(00000041302>813253000000000075000073337+ 012000159>

Source : santésuisse - http://www.santesuisse.ch/datasheets/files/200608091418300.pdf

Annexe 2
Code diagnostics

Codes diagnostics pour traitements ambulatoires

1. Code principal

A. Système cardio-vasculaire

A 1 Vitiens cardiaques/ valvules cardiaques
A 2 Maladies coronariennes, y compris infarctus du myocarde
A 3 Troubles du rythme cardiaque
A 4 Hypertonie artèrielles
A 5 Artères
A 6 Veines (y compris varices)
A 7 Vaisseaux lymphatiques y compris œdème lymphatique
A 9 Autres maladies du système cardio-vasculaire

B. Sang / moelle osseuse/ rate

B 1 Anémie
B 2 Coagulopathie
B 3 Maladies de la moelle osseuse et du sang
B 4 Rate / ganglion lymphatique / système immunitaire
B 9 Autres maladies de la moelle osseuse / du sang / de la rate

C. Poumon / appareil respiratoire

C 1 Asthme
C 2 Bronchite chronique
C 3 Embolie pulmonaire
C 4 Poumon / plèvre (tuberculose exclue)
C 9 Autres maladies de l'appareil respiratoire

D. Squelette / appareil locomoteur

D 1 Muscles / tendons
D 2 Articulations / ligaments / bourse (D3 exclu.)
D 3 Arthrite / M. Bechterew
D 4 Arthrose
D 5 Colonne vertébrale (D3 exclu.)
D 9 Autres maladies de l'appareil locomoteur

E. Tube digestif

E 1 Oesophage / estomac / duodénum, ulcère compris)
E 2 Intestin (intestin grêle / colon)
E 3 Rectum / anus, hémorroïdes comprises)
E 4 Foie / voies biliaires / vésicule biliaire
E 5 Pancréas, diabète exclu)
E 6 Diaphragme
E 7 Hernies
E 9 Autres maladies du tube digestif

F. Métabolisme

F 1 Métabolisme glucidique
F 2 Maladies de la glande thyroïde
F 9 Autres maladies du métabolisme

G. Maladies infectieuses et parasitaires

G 1 Infection banale
G 2 Tuberculose
G 3 Hépatite virale
G 9 Autres maladies infectieuses ou parasitaires

H. Rein et voies urinaires

H 1 Rein / insuffisance rénale (dialyse / transplantation)
H 2 Calcul rénal
H 3 Voies urinaires
H 9 Autres maladies des reins et des voies urinaires

I. Organes génitaux

I 1 Organes génitaux masculins
I 2 Vulve, vagin, petit bassin
I 3 Utérus
I 4 Annexes
I 5 Troubles du cycle menstruel
I 6 Maladies de la glande mammaire
I 7 Stérilisation
I 9 Autres maladies des organes génitaux

K. Grossesse / stérilité

K 1 Grossesse risque normal
K 2 Grossesse avec complications
K 3 Stérilité et insémination artificielle

L. Système nerveux

L 1 Cerveau / moelle épinière
L 2 Nerfs périphériques
L 3 Paralysie / ataxie
L 4 Migraine et équivalents
L 5 Epilepsie
L 9 Autres maladies du système nerveux

M. Maladies psychiques

M 1 Troubles du sommeil
M 2 Maladies psychiques
M 3 Maladies psycho-organiques

N. Peau

N 1 Maladies allergiques de la peau, eczéma exclu.
N 2 Maladies inflammatoires / infectieuses de la peau
N 3 Eczéma
N 4 Maladies vasculaires / dégénératives de la peau
N 5 Psoriasis / hyperkératoses
N 6 Cicatrices
N 9 Autres maladies de la peau

O. Cou / nez / oreilles

O 1 Nez, N6 exclu.
O 2 sinus nasal
O 3 Cavité buccale, glandes salivaires
O 4 Amygdales / adénoïdes
O 5 Larynx / trachée
O 6 Malformations du nez et des oreilles
O 7 Oreille moyenne / trompe d'Eustache
O 8 Oreille interne
O 9 Autres maladies ORL

P. Oeil

P 1 Paupière / conjonctive
P 2 Lentille / cornée / corps vitré
P 3 Iris / glaucome
P 4 Rétine / nerf optique / vaisseaux
P 5 Muscle oculomoteur / strabisme
P 9 Autres maladies des yeux

Q. Dents / mâchoire

Q 1 Kyste
Q 2 Abcès dentaire
Q 3 Fibromes
Q 9 Autres maladies de la mâchoire ou dentaires

R. Accident / conséquences de l'accident

R 1 Tête / colonne vertébrale
R 2 Thorax
R 3 Abdomen
R 4 Extrémités supérieures
R 5 Extrémités inférieures

S. Prestations non prises en charge par l'assurance-maladie

T. Mesures préventives

T 1 Examen préventif
T 2 Vaccins

U. Orientation du médecin-conseil (au lieu du diagnostic)

2. Codes supplémentaires

Plusieurs indications sont possibles, si nécessaire.

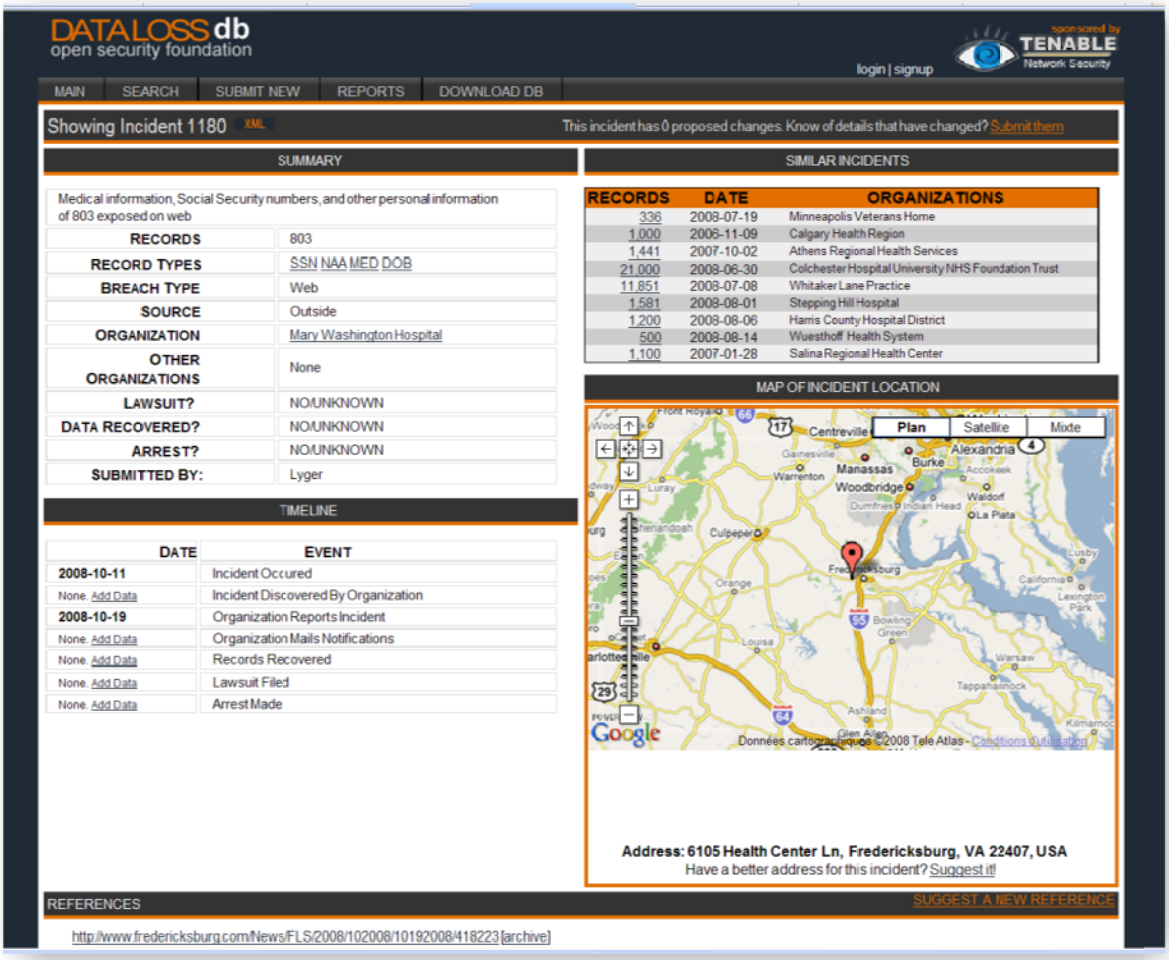
01	droite
02	gauche
03	aigu
04	chronique / récidive
05	infectueux
06	fonctionnel
07	néoplasie
08	raisons professionnelles

Interprétations

« Plusieurs chiffres du code principal peuvent être indiqués. En cas d'utilisation du code supplémentaire, le code principal doit également être indiqué. Le code principal et le code supplémentaire doivent toujours être indiqués pour les néoplasies. Les lésions corporelles assimilées aux accidents au sens de l'article 9 alinéa 2 LAA / OLAA doivent être attribuées au code principal R. ***Par code U, on entend la communication du diagnostic précis au médecin-conseil compétent. Celui-ci est obligatoire en cas de séquelles après des tentatives de suicide.*** *Au cas où une facture comporterait une prestation non obligatoire, celle-ci doit être munie d'une étoile (*). En cas d'infections, le code principal correspondant désigne l'organe touché et le code supplémentaire le précise (exception groupe G / N2). »*

Source : http://www.fmh.ch/shared/data/pdf/annexe4b_diagnostic.pdf

Annexe 3
DATALOSSdb



Source : http://datalossdb.org/incidents/1180

Annexe 4
Profils des droits d'accès du DPI

Profil	Droits applicatifs	Commentaires et usage
Infirmier	Consultation sur DPI-Modules médicaux (résultats de laboratoire, rapports de consultants, infos du dossier social, etc.) Ecriture dans DPI-Mi	Accès réservé uniquement aux patients actifs dans DPA pour son unité de soins. Pas d'accès en dehors de sa zone d'activité de soins (par « vitre brisée »).
Infirmier non-référent	Mêmes droits que les infirmiers, mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	A réserver pour les infirmières des équipes de remplacement HUG ou intérimaires d'agence.
Infirmier étudiant	Mêmes droits que les infirmiers mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	Case à cocher dans l'écran d'octroi du droit dans DPI-Mi
Sage - femme	Consultation sur DPI-Modules médicaux (résultats de laboratoire, rapports de consultants, infos du dossier social, etc.) Ecriture dans DPI-Mi	Accès réservé uniquement aux patients actifs dans DPA pour son unité de soins. Pas d'accès en dehors de sa zone d'activité de soins (par « vitre brisée »).
Sage – femme étudiante	Mêmes droits que les sages-femmes, mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	Case à cocher dans l'écran d'octroi du droit dans DPI-Mi
Sage – femme non référente	Mêmes droits que les sages-femmes, mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	A réserver pour les sages-femmes des équipes de remplacement HUG ou intérimaires d'agence.
Aide soignant	Consultation sur DPI-Modules médicaux (résultats de laboratoire, rapports de consultants, infos du dossier social, etc.) Ecriture dans DPI-Mi **Pas de possibilité d'effectuer un « mouvement » du dossier** (création, cloture d'un dossier sur DPI).	Accès réservé uniquement aux patients actifs dans DPA pour son unité de soins. Pas d'accès en dehors de sa zone d'activité de soins (par « vitre brisée »).
Aide soignant étudiant	Mêmes droits que les aides soignants, mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	Case à cocher dans l'écran d'octroi du droit dans DPI-Mi
Aide soignant non référent	Mêmes droits que les aides soignants, mais le nom n'apparaît pas dans la liste des référents (onglet « informations de DPI-Mi)	A réserver pour les aides soignants des équipes de remplacement HUG ou intérimaires d'agence.

Cadres infirmiers :

Infirmière spécialiste clinique	Mêmes droits que les infirmiers	Le droit d'accès doit être demandé par la DSI et autorisé par le médecin chef de service concerné. **Il est fait mention par le DOOP de cette autorisation** et de la date de celle-ci, dans la rubrique « informations complémentaires» du logiciel d'octroi des droits.
Infirmier chargé d'études	Droits de consultation uniquement des dossiers sur le DPI-Modules médicaux et infirmiers	Le droit d'accès doit être demandé par la DSI et autorisé par le médecin chef de service concerné. **Il est fait mention par le DOOP de cette autorisation** et de la date de celle-ci, dans la rubrique « informations complémentaires» du logiciel d'octroi des droits.
Infirmier IAG	Droits de consultation uniquement des dossiers sur le DPI-Modules médicaux et infirmiers	Accès réservé uniquement au(x) service(s) médical(ux) de sa zone d'activité.
Infirmier & Sage-femme/homme formateur / moniteur	Droits de consultation uniquement des dossiers sur le DPI-Modules médicaux et infirmiers	Accès réservé uniquement au(x) unité(s) de soins de sa zone d'activité.
« Infirmier de gestion et d'enseignement » : ⇨ pour AICO ⇨ pour ICO ⇨ pour Direction des soins	Droits de consultation uniquement des dossiers sur le DPI-Modules médicaux et infirmiers	Accès réservé uniquement au(x) service(s) médical(ux) de sa zone d'activité. Pour les professionnels hors service médical concerné, le droit d'accès doit être autorisé par le médecin chef de service concerné. **Il est fait mention par le DOOP de cette autorisation** et de la date de celle-ci, dans la rubrique «informations complémentaires ».

Source : Lettre de la direction générale – Groupe des droits d'accès