Sécurité dans les Systèmes Médicaux Informatisés

Dr. Ross Anderson

Computer Laboratory, University of Cambridge
Pembroke Street, Cambridge CB2 3QG

Janvier 1996

Note du traducteur

Ce document, publié le 12 Janvier 1996 par la *British Medical Association* (BMA), établit un certain nombre de règles assurant le principe de consentement du malade. Une version plus technique a été présentée au symposium de 1996 organisé par l'*Institute of Electrical and Electronics Engineers* (IEEE).

Suite à ces publications et aux divergences entre le *National Health Service* (NHS) et la *British Medical Association* une conférence de travail a été organisée en juin 1996 à Cambridge et a permis de confirmer les principes énoncés ci-après.

Nota : Certains passages n'ont volontairement pas été traduits ; mais les versions complètes de ces documents sont disponibles sur Internet à l'adresse suivante : `http://www.cl.cam.ac.uk/users/rja14/#Med`

Fabien Petitcolas

Sécurité dans les Systèmes Médicaux Informatisés

Dr. Ross Anderson

Computer Laboratory, University of Cambridge
Pembroke Street, Cambridge CB2 3QG

Janvier 1996

1 Introduction

L'introduction en Grande Bretagne par le National Health Service (NHS) d'un réseau informatique médical national a conduit l'auteur à s'intéresser à la sécurité d'un tel système. Médecins et Professionnels de Santé s'inquiètent d'une plus grande disponibilité des informations médicales personnelles qui pourrait mettre en danger la vie privée des patients [ACH95]. Le problème ne se limite pas seulement au NHS ; il affecte également les cliniques carcérales, les services d'immigration, les laboratoires médico-légaux et la médecine privée. Le réseau du NHS a permis de bien mettre en évidence ces problèmes.

Il a généralement été admis que la sécurité accordée aux dossiers électroniques des patients doit au moins égaler, si ce n'est dépasser, celle appliquée aux dossiers papiers habituels ; mais là encore le manque de clarté sur les objectifs de protection a conduit à une certaine confusion. La British Medical Association (BMA) a, par conséquent, demandé à l'auteur de considérer les risques possibles, et de préparer une politique de sécurité pour les systèmes médicaux d'information.

1.1 Champ de la politique

Une politique de sécurité doit indiquer *qui* peut accéder à *quelle information* ; par accès, on entend la lecture, l'écriture, l'ajout et l'effacement d'informations. Cette politique découle d'un modèle des menaces subies par le système et dicte certains aspects de la conception de ce dernier. Pour être efficace, cette politique doit être écrite au bon niveau d'abstraction ; elle ne doit pas embarrasser le lecteur avec des détails inutiles sur des équipements particuliers. Elle doit adresser pleinement les problèmes importants et ignorer les digressions.

Une digression potentielle est la signification précise de « patient, » « médecin » et « système. » On pourrait s'étendre longuement sur ce qui

pourrait se passer quand un médecin délègue certaines tâches à un étudiant, ou lorsque le patient est un mineur ou une personne décédée. Ces questions peuvent être difficiles mais ne sont pas importantes dans le cadre de la politique de sécurité elle-même ; nous clarifions donc ces termes dès maintenant plutôt que dans le corps de la politique.

1.2 Définitions

Par « **information personnelle de santé**, » ou de façon équivalente « **information clinique identifiable**, » nous rassemblons toute information concernant la santé d'une personne, son passé médical ou ses traitements (passés ou futurs) sous une forme qui permet d'identifier cette personne par une autre personne, différente du clinicien traitant [RAC93].

Par « **médecin**, » ou « **professionnel de santé**, » nous entendons tous les professionnels autorisés comme les médecins, les infirmières, les dentistes, les psychothérapeutes ou les pharmaciens, qui, de par leurs fonctions, ont accès à des informations personnelles de santé et sont soumis au secret professionnel.

Le lecteur peut consulter la loi britannique de 1990 concernant l'accès aux dossiers médicaux pour une définition légale de « professionnel de santé, » mais doit être averti qu'elle prête à controverse : le débat porte sur l'inclusion ou non, à l'intérieur de la limite de confiance, des psychothérapeutes, des employés donnant des conseils par téléphone, des praticiens de médecine complémentaire et autres employés des services sociaux. Quoi qu'il en soit cette limite existe quelque part et sa position précise n'a que peu d'influence sur notre politique. Les employés des services sociaux ou des associations caritatives, les étudiants, les réceptionnistes peuvent bien sûr avoir accès à des informations personnelles de santé mais sous la surveillance d'un professionnel de santé qui reste responsable de leur conduite. Pour garder les choses simples, nous ne tenons pas compte de telles délégations dans notre politique ; mais au niveau des détails de conception, il est judicieux pour les développeurs de systèmes d'information de supporter la délégation de façon intelligente.

Notre utilisation du mot « **patient** » est un raccourci pour « l'individu concerné ou le représentant de l'individu, » au sens du projet de loi déposée par la British Medical Association [BMA95]. Dans la plupart des cas il s'agit du véritable patient ; mais si le patient est un jeune enfant, son tuteur légal décidera à sa place. Il existe des règles pour les patients qui sont inconscients ou décédés, et des règles encore plus complexes pour les patients ayant des troubles d'ordre mental. Ces règles peuvent dépendre des souhaits précédemment exprimés par les patients et varient suivant les régions de Grande Bretagne [Som93]. Nous détaillons ces problèmes un peu plus loin.

Par « **système** » nous englobons l'ensemble des équipements informatiques — matériel, logiciels, moyens de communication, procédures manuelles — qui constituent un système connecté de traitement de l'information. Nous ne sommes pas concernés ici par ce qui constitue réellement le système : un gros ordinateur auquel sont connectés des centaines de terminaux, un réseau de micro-ordinateurs personnels reliés par une série de protocoles et d'applications distribuées ou même un millier d'employés s'échangeant des informations sur papier. Nous nous intéressons seulement aux effets découlant du traitement de l'information ; c'est aussi le sens de la récente Directive Européenne concernant la protection des données [EU95].

Il devrait être clair dans ce contexte si nous parlons de l'ensemble du système interconnecté ou d'un sous ensemble utilisé par un individu particulier ou une équipe de soins.

1.3 Mises en garde

Tout d'abord ce document adresse seulement les aspects médicaux de la sécurité des informations. Il ne considère pas les aspects commerciaux associés comme la confidentialité des contrats pouvant exister entre acheteur et fournisseur et la validité légale des dossiers électroniques devant une cour de justice.

Ensuite nous ne nions pas que l'informatisation des dossiers médicaux pourrait apporter des gains en matière de sécurité : chiffrer les dossiers en transit permet d'obtenir une confidentialité beaucoup plus forte que celle offerte par les services postaux ; les systèmes de détection d'intrusion peuvent garder les traces de tous les accès et les analyser par la suite pour révéler les comportements douteux ; une sauvegarde des données sur un autre site peut protéger efficacement et économiquement contre un feu ou une inondation.

Cependant nous devons d'abord comprendre nos priorités en matière de protection avant que ces techniques puissent être appliquées et une politique de sécurité est un pas important dans ce sens.

2 Menaces et vulnérabilités

Dans cette section, nous décrivons les menaces dues à l'informatisation auxquelles est sujette la sécurité d'un système de santé ; en particulier l'interconnexion d'un grand nombre d'ordinateurs sur lesquels sont stockés les dossiers médicaux des patients de plusieurs hôpitaux. Tout d'abord nous passons en revue les objectifs de la politique, ensuite nous

considérons les problèmes qui peuvent survenir, et enfin, nous établissons la liste de nos priorités.

2.1 Les bases éthiques de la confidentialité

Le serment d'Hippocrate intègre le principe de confidentialité de l'information médicale dans le code déontologique des médecins. Une version moderne de cette déclaration est donnée dans « Good Medical Practice[1] » [GMC1] publié par le General Medical Council (GMC) :

> *Les patients ont le droit d'attendre de vous, que vous ne divulguerez aucune information personnelle que vous aurez apprise au cours de votre activité professionnelle sans leur consentement.*

Ceci est développé dans une brochure d'information publiée par le GMC [GMC2]. Elle stipule, que les médecins qui enregistrent ou conservent des informations confidentielles, doivent s'assurer que ces informations sont efficacement protégées contre toute divulgation malhonnête. Un guide encore plus détaillé a été publié par la British Medical Association [Som93] et l'HMSO[2] [DGMW94].

Le Gouvernement Britannique ainsi que les unions de santé sont d'accord sur un point : les dossiers électroniques doivent être protégés au moins aussi bien que leur équivalent papier ; la loi britannique sur la protection des données (Data Protection Act) rend les médecins responsables de la sécurité des informations personnelles de santé qu'ils collectent ; une récente Directive Européenne force le Gouvernement à interdire le traitement des données de santé lorsque le sujet n'a pas donné sont consentement explicite ainsi que dans certaines autres circonstances [EU95]. Le principe de base établi par le General Medical Council et l'Union Européenne, est que le patient doit donner son consentement pour le partage des données. La confidentialité est le privilège du patient, qui seul, peut y renoncer [DGMW94] ; et le consentement doit être informé, raisonné et volontaire [Som93]. Ainsi, par exemple, les patients doivent être avertis que l'information les concernant peut être partagée entre les membres d'une même équipe de soins d'un centre un hospitalier.

Un certain nombre d'exceptions à cette règle ont été développées au cours du temps. Elles incluent des exigences statutaires et des exemptions réclamées pour des raisons pratiques ; elles concernent les notifications d'avortement, les naissances, certains cas de décès, certaines maladies, les allergies aux médicaments, les blessures non accidentelles, l'aptitude à conduire et les divulgations à des avocats dans le cadre d'un procès

---

[1] Bonnes pratiques en Médecine.

[2] *Her Majesty's Stationery Office* : l'éditeur officiel du Gouvernement de Grande Bretagne.

[DGMW94]. Des controverses existent en ce qui concerne la Recherche ; les représentants du NHS affirment qu'en acceptant le traitement, un patient donne son consentement implicite pour l'utilisation de son dossier médical dans les activités de recherche, tandis que les Professions Médicales n'acceptent pas cette présomption [Mac94]. Quoi qu'il en soit ce débat n'a pas beaucoup d'effets sur la politique développée ici.

Finalement, il reste la question de demander ou non le consentement du patient pour informatiser son dossier médical. Il n'est pas éthique d'établir une discrimination contre un patient souhaitant que son dossier soit conservé sur papier ; ses craintes peuvent être justifiées s'il est une célébrité, ou une cible pour un attentat, ou pour toute autre raison pour laquelle il serait en danger. Certains cas de ce genre ont été résolus en utilisant un pseudonyme, de telle façon que la véritable identité du patient n'est jamais entrée dans le système informatique.

2.2 D'autres besoins en matière de sécurité

Deux autres exigences viennent s'ajouter à la confidentialité des systèmes d'information pour la Santé : l'intégrité et la disponibilité.

Si l'information fournie par le système est erronée, le médecin peut prendre des décisions causant du tort au patient, ou pire, le tuant. Si l'information n'est pas fiable, en ce sens qu'elle aurait pu être corrompue (même si ce n'est pas le cas), sa valeur comme base de diagnostique est amoindrie. De plus, dans le cadre médico-légal, un professionnel de la santé appelé à justifier ses actions pourrait être dans l'incapacité d'utiliser les dossiers informatisés comme preuve ; d'ailleurs, est-il suffisant d'utiliser uniquement les dossiers sous forme électronique ou doit-on garder des copies de secours sous forme de microfiches ou de dossiers papier ?

Les systèmes d'information ne sont également pas fiables dès lors qu'une l'information existante peut ne pas être disponible suite à une panne du système informatique, ou un sabotage. Dans ce cas aussi la valeur des dossiers informatisés est diminuée et l'utilisation qui peut en être faite prudemment est restreinte.

Il est donc prudent de s'interroger sur les méthodes qui peuvent garantir l'intégrité des dossiers et empêcher des attaques qui pourraient compromettre la disponibilité du système.

2.3 Menace à l'égard de la confidentialité

Beaucoup d'organisations, à la foi publiques et privées, ont remplacé leurs dossiers, dispersés et tenus manuellement, par des systèmes informatiques centralisés leur offrant un meilleur accès aux données.

Leurs expériences montre que la menace la plus importante vient de l'intérieur. Par exemple, la plupart des grandes banques de Grande Bretagne laissent n'importe quel caissier accéder à n'importe quel compte ; les journaux rapportent que des détectives privés soudoient des caissiers pour obtenir des informations bancaires vendues environ mille francs [LB94]. Cette pratique a récemment été rendue illégale par un amendement de la loi sur la protection des données, mais, à notre connaissance, il n'y a toujours pas eu de poursuites judiciaires.

Les effets de l'agrégation des données dans de grandes bases de données auraient dû être prévus. La probabilité pour qu'une information soit divulguée à tort dépend de deux choses : sa valeur et le nombre de personnes qui y ont accès. L'agrégation des dossiers augmente en même temps ces deux risques. Elle crée également une ressource précieuse sujette à des pressions politiques motivées par un besoin de savoir [Smu94].

Les systèmes de Santé n'échapperons certainement pas à ces problèmes. Actuellement, la sécurité dépend de la fragmentation et de la dispersion inhérentes aux systèmes basés sur le papier ; ces systèmes sont très vulnérables, par exemple, aux détectives privés téléphonant en prétendant appartenir à un autre hôpital. Une récente enquête a montré que la plupart des dossiers médicaux pouvaient être obtenus pour seulement 1 500 francs [RL95]. Il existe aussi des incidents impliquant l'informatique :

- à la suite d'un vol d'ordinateurs dans un cabinet médical, deux femmes occupant des positions importantes reçoivent des lettres anonymes les menaçant de rendre public leur avortement ;
- il existe un abus continuel des ordonnances [JHC94] ;
- un maniaque sexuel se faisant appeler « Docteur Jackson » gagne la confidence de jeunes femmes en leur parlant de leur antécédents familiaux par téléphone et essaye, par la suite, d'organiser une entrevue. La Police pense qu'il est un employé d'un service de santé ou un pirate informatique [Tho95].

Un guide provisoire publié en même temps que cette politique explique comment de telles attaques, que ce soit des systèmes informatiques ou papier, sont possibles. Les risques sont aujourd'hui limités car les réseaux existant en Grande Bretagne ont un champ d'applications également limité (géographiquement ou par fonction). L'introduction d'un réseau informatique national augmenterait sérieusement le nombre de torts causés.

Autrement dit, il n'est pas très préoccupant de savoir que la secrétaire d'un médecin ait accès aux dossiers de 2 000 patients ; en revanche que les 32 000 secrétaires aient accès aux dossiers de 56 000 000 de patients l'est

beaucoup plus. Le danger de l'agrégation des dossiers médicaux et la vraisemblance selon laquelle des abus en résulteront, sont confirmés par l'expérience des États-Unis où l'informatisation et l'utilisation des réseaux sont un peu plus avancées qu'en Grande Bretagne :

- un sondage Harris sur la confidentialité de l'information médicale montre que 80% des personnes interrogées doutent de cette confidentialité, et qu'un quart d'entre elles ont déjà été victimes d'abus [GTP93].
- quarante pour-cent des assureurs divulguent des informations privées à des prêteurs, des employeurs ou des entreprises commerciales sans la permission des personnes concernées [CR94] ; et plus de la moitié des 500 plus grandes compagnies américaines reconnaissent utiliser des dossiers médicaux lorsqu'elles doivent prendre certaines décisions et notamment l'embauche d'un employé [Bru95] ;
- un banquier membre d'une commission de santé a eu accès à la liste de l'ensemble des patients victimes du cancer dans son État. Il a croisé cette information avec la liste de ses clients ayant demandé un prêt [HRM93] ;
- une compagnie pharmaceutique américaine a pu avoir accès à une base de données contenant les ordonnances de 56 millions de personnes simplement en achetant une compagnie de systèmes de santé. Après en avoir extrait la liste des patients pouvant être dans un état de dépression, se manifestant par des maux de tête ou un manque de sommeil, elle tente de convaincre leurs médecins de leur prescrire Prozac [See95] ;
- une agence vérifiant la solvabilité de clients désireux de souscrire un emprunt est en train de construire un réseau pour échanger des dossiers médicaux. Elle soutient également un projet de loi du Congrès Américain qui faciliterait l'échange de données médicales entre parties intéressées et retirerait aux patients le droit de poursuivre en justice ces compagnies en cas de problème. C'est un exemple conduisant à des pressions politiques en vue d'obtenir un accès légitime à des données ; accès vivement contesté par les associations de patients ou les défenseurs de nos libertés.

Le problème a été étudié par le l'Office of Technology Assessment (bureau d'évaluation des technologies) du Gouvernement Américain. Il confirme, que la plus grande menace pour les dossiers médicaux informatisés, est due essentiellement, à des personnes habilitées plutôt qu'à des personnes sans lien avec le système, et que ces menaces sont amplifiées par l'agrégation, elle même favorisée par les réseaux informatiques [OTA93]. Le besoin de savoir grandissant et les traitements, influencés en fonction des intérêts d'une entreprise partenaire plutôt que du patient, vont de paire avec l'agrégation des données [Woo95].

Le Gouvernement Britannique reconnaît qu'un large accès à des dossiers médicaux identifiables n'a pas de base éthique. Pas même un médecin ne devrait avoir accès aux informations personnelles de santé sans véritable nécessité. Selon David Bellamy, membre du Comité Directeur au Ministère de la Santé :

> *Une idée communément admise [...] veut, qu'en tant que médecin, je puisse discuter avec un autre médecin du cas d'un patient parce qu'un médecin est soumis au secret en raison de ses obligations éthiques. C'est tout à fait faux et cela ne tient pas la route. Même si cela peut être utile pour un médecin de discuter avec un collègue du cas d'un patient, il ne doit le faire que sur la base des informations strictement nécessaires à ce collègue* [WHC95].

Fréquemment des assureurs, des employés de services sociaux, des policiers et des administrations affirment qu'ils ont « besoin de savoir » certaines informations personnelles concernant la santé d'une personne. En examinant de telles réclamations, il peut être utile de se rappeler que la nécessité d'avertir un chirurgien que sont patient est atteint du virus du SIDA — afin qu'il prenne des précautions supplémentaires — n'est pas suffisante pour ne plus garantir la confidentialité qu'est en droit d'attendre le patient. Un cas de Justice à même montré qu'il n'était pas nécessaire de divulguer l'état séro-positif d'un médecin : le petit risque encouru par ses patients ne contrebalance pas l'intérêt public du maintien du secret qui permet à ces personnes de rechercher de l'aide [DGMW94].

La British Medical Association n'admet pas que le « besoin de savoir » puisse être une raison suffisante pour accorder l'accès à des informations relevant de la vie privée. Des documents publiés par l'Union Européenne et le General Medical Council établissent clairement que seul le consentement du patient a une importance dans ce domaine. Ce concept de « besoin de savoir » implique et encourage une érosion subreptice des privilèges des patients par simple convenance administrative. Dans tous les cas le besoin ne confère pas des droits : la Police a besoin de savoir si un suspect dit la vérité mais cela ne lui donne pas le droit à la torture. Il est également bon de garder à l'esprit les études empiriques montrant la forte résistance des patients à confier des informations privées sur leur état de santé à des employés du National Health Service ou des Services Sociaux ou encore des statisticiens du Gouvernement [Haw95].

2.4 D'autres menaces envers l'information médicale

En plus des menaces pouvant compromettre la confidentialité de l'information médicale, l'intégrité et la disponibilité de cette dernière peuvent aussi être en péril dans un système informatisé, et souvent de façons qui n'apparaissent pas immédiatement.

- Les erreurs de programmation ou de conception (« bugs ») des logiciels ou les défaillances du matériel informatique corrompent occasionnellement des messages. Bien que la poste, les fax ou les systèmes téléphoniques commettent des erreurs, ces dysfonctionnements sont plus évidents que ceux apparaissant dans les systèmes informatisés. Il est tout à fait possible, par exemple, qu'un « bug » puisse altérer des résultats numériques dans un rapport de laboratoire sans pour autant éveiller l'attention.
- Régulièrement la Presse cite des cas de frottis cervicaux trompeurs et d'avortements décidés à tort, pensant que le foetus était atteint du syndrome de Down. Nous ne savons pas combien de cas sont dus à des erreurs du système informatique lui même, par opposition à des erreurs humaines ; mais l'expérience acquise dans d'autres secteurs montre qu'en l'absence de contrôles sévères d'intégrité, environ un message sur 10 000 peut être erroné. Pour un médecin généraliste, cela voudrait dire un mauvais résultat environ tous les cinq ans et un traitement dangereux durant sa carrière. Avec des logiciels de conception médiocre, ces chiffres pourraient augmenter de façon considérable.
- L'utilisation de courriers électroniques (emails) non structurés et interprétés par la machine se traduirait par des taux d'erreur encore plus élevés. Un scénario comme celui proposé dans [Mar95] est tout à fait plausible : un employé de laboratoire ajoute un commentaire avant un résultat numérique, mais le système informatique du médecin partant du principe que la première valeur qu'il rencontre est le résultat, ajoute celle ci au dossier du patient ; ce qui conduit à un mauvais traitement.
- Les virus informatiques ont déjà détruit des informations médicales ; ils pourraient très bien être écrits pour altérer malicieusement des dossiers médicaux.
- Une personne malintentionnée pourrait également manipuler les messages. Envoyer un courrier électronique avec une adresse d'envoyeur factice est facile et avec un peu plus d'effort il est possible d'intercepter un message entre deux correspondants et de le modifier.
- Toutefois, ce sont bien des personnes ayant accès, de par leur profession, à des données confidentielles, qui, en majorité, utilisent de façon malveillante le système d'information [OTA93] : effacement de dossiers montrant des négligences [Ald95], additions ou remplacements, vol manifeste ou escroquerie. L'utilisation frauduleuse d'ordonnances existe déjà

dans les systèmes manuels et, en l'absence de meilleurs contrôles, ne pourra que s'accroître.

- Une érosion de la confidentialité rend plus probables les attaques perpétrées contre l'intégrité d'un système : si les dossiers médicaux devenaient largement accessibles et étaient utilisés, par exemple, pour embaucher ou accorder un crédit bancaire (comme c'est le cas aux États-Unis [Woo95]) il y aurait alors de bonnes raisons pour les altérer.
- Le manque de confiance du publique dans ces systèmes d'information pourrait également dégrader la qualité des données enregistrées puisque certains patients ne divulgueraient pas des informations néanmoins nécessaires. Les craintes du publique américain ont atteint un tel niveau que certains journaux ont mis en garde leurs lecteurs pour qu'ils divulguent des informations sensibles avec prudence [USA95].
- Des effets similaires pourraient être constatés si une partie des informations médicales étaient utilisées à d'autres fins que la Santé. Par exemple, si la carte de santé venait à être utilisée comme carte d'identité [DPR95], alors criminels et défenseurs extrémistes des libertés essayeraient de briser sa sécurité et les patients partiraient du principe que la Police a accès à ces informations, et ce, malgré les assurances du Gouvernement.

Pour toutes ces raisons, la confidentialité et l'intégrité des systèmes informatiques de Santé ne devraient pas être considérées isolément.

2.5 Protections par ordre de priorité

Une erreur courante dans l'étude de la sécurité des systèmes informatiques, est de ce concentrer sur les menaces « fascinantes », mais rares, comme les écoutes indiscrètes par des services secrets étrangers qui pourraient par exemple décoder les radiations électromagnétiques émanant d'un écran d'ordinateur. Bien que de telles attaques soient possibles, elles ne sont pas, en pratique, prises en compte, étant donné qu'un adversaire déterminé trouvera des méthodes moins coûteuses et plus sûres pour obtenir cette information (cambriolage ou corruption, par exemple).

Un autre exemple est la publicité faite par les médias aux pirates de l'informatique sur le réseau Internet. Il est vrai qu'une personne avisée peu manipuler le trafique de différentes manières et pourrait parvenir à s'infiltrer dans un système informatique en « flairant » des mots de passe et en falsifiant son adresse. Toutefois, de telles attaques sont rares et un fournisseurs d'accès à Internet compétent mettra en place des systèmes de

protection[3] les rendant très difficiles. Un risque beaucoup plus grand est tout simplement le vol de matériel informatique dans un hôpital ou un cabinet médical ; environ 10% des médecins généralistes ont déjà été victimes de vols d'ordinateurs [PK95].

Nous devons par conséquent faire la distinction entre vulnérabilité (les choses qui pourraient mal se passer) et les menaces (les problèmes qui vont certainement survenir).

Nous mesurerons l'impact des menaces par le nombre d'individus pouvant être concernés. Il existe des menaces internationales pouvant affecter le caractère privé, l'intégrité ou la disponibilité des informations personnelles de santé de l'ensemble de la population, comme le marché noir existant ; pourtant la plupart des menaces ont un caractère local et affectent seulement les dossiers conservés par une équipe de soin : vols d'équipement, feu, virus informatiques et divulgation à des tiers par des employés peu scrupuleux. Ces menaces locales peuvent être minimisées en utilisant des techniques plus ou moins bien maîtrisées : formation du personnel, sauvegardes des données sur un autre site et audits réguliers par des organismes indépendants ; l'essentiel des efforts faits pour augmenter la sécurité des données dans les cabinets médicaux ou les unités de soin des hôpitaux leur seront consacrés. Des directives générales ont été distribuées par le Department of Health[4] [NHS95] ; la British Medical Association a également publié ses propres directives [And96] concernant les mesures devant être prises pour contrecarrer les menaces les plus sérieuses et dont nous connaissons l'existence à cette date. Entre temps notre tactique consiste d'abord à nous assurer que des attaques locales ne puissent pas s'étendre ou ne puissent pas en renforcer d'autres déjà répandues, à cause d'une agrégation inconsidérée des données ou de la négligence du principe de consentement. Les principes de sécurité que nous souhaiterions appliquer dans tous les systèmes informatiques médicaux utilisant des réseaux de communication doivent d'abord adresser les problèmes d'agrégation et de consentement.

2.6 Exemples d'agrégation dans le système proposé par le National Health Service

L'agrégation des informations personnelles de santé peut se produire de différentes façons, certaines pleinement justifiées et d'autres obéissant à des pressions sans grand rapport avec la Santé. Par exemple au moins deux systèmes qui ont été développés permettent aux Autorités de Santé de faire le lien entre ordonnances, demandes de remboursement et

[3] Par exemple des « firewalls » (littéralement « murs de feu »).
[4] Ministère de la Santé en Grande Bretagne.

d'autres données contractuelles afin de créer un « dossier fantôme » en dehors de tout contrôle médical [AIS95] [DL95].

Ces systèmes ont été adoptés malgré un accord, entre la Direction du National Health Service et les Syndicats de Médecins, selon lequel les dossiers électroniques seraient au moins aussi protégés que leur équivalent papier et malgré d'autres directives[5] soulignant clairement l'importance de ne pas pouvoir identifier un patient — à moins d'être son médecin — à partir de n'importe quelle donnée envoyée à des organismes extérieurs, sans en avoir informé celui-ci [JCG88].

Un objectif stratégique de la Direction Informatique du National Health Service est une base de données entièrement partagée sur les patients ; nous présumons que la collecte des données conservées par les médecins généralistes est l'élément directeur et que les ordinateurs de ces médecins seront interrogés par ceux du National Health Service. Pourtant ces objectifs sont clairement en contradiction avec la déontologie adoptée par la British Medical Association [Som93]. Le consentement des patients, pour communiquer au National Health Service, des informations privées concernant leur santé, n'est pas pris en compte ; d'ailleurs une étude montre que la plupart d'entre eux n'y sont pas favorables [Haw95].

Accumuler des informations sensibles dans de larges bases de données, qui sont même en dehors du contrôle des professionnels de Santé, est extrêmement dangereux ; comme le montre l'expérience Américaine, la simple existence de telles ressources ayant une valeur potentielle importante, ne peut qu'engendrer des pressions politiques pour autoriser l'accès à des compagnies d'assurances, des agences chargées de faire respecter la loi, et bien d'autres.

La réponse de la British Medical Association comprend ce document. Son but premier et d'aider les médecins et professionnels de la Santé à s'acquitter de leurs responsabilités légales et éthiques en choisissant des systèmes informatisés appropriés et en les utilisant de façon sûre. Nous avons essayé de définir à quel genre de système on peut prudemment confier des informations médicales. Pour ces systèmes, nous développons une politique de sécurité basée sur le modèle des menaces exposé précédemment. Cette politique consiste en un petit ensemble de règles, qui, si elles sont mises en œuvre correctement, ferons respecter efficacement le consentement du patient.

[5] Directives proposées par un groupement informatique commun au General Medical Services (organisme payant les médecins généralistes) et au Royal College of General Practitioners.

3 Politique de sécurité

Le principe de consentement et les règles utilisées pour l'interpréter sont bien établies — elles ont évolué avec l'expérience séculaire de la Médecine, et sont soutenues par la loi sur la protection des données informatiques. Dans cette section nous les rassemblons sous la forme d'une politique de sécurité — un ensemble de principes décrivant quel sujet peut accéder à quel objet dans un système informatisé. Ces règles n'ont rien de radicalement nouveau, mais elles reformulent des principes de bon sens dans le langage moderne utilisé en sécurité informatique.

Cette politique couvre les systèmes informatiques médicaux en général. Certains médecins souhaiterons peut-être y ajouter des règles, et ceux qui traitent plus d'un patient à la foi (psychiatres pour enfants, embryologistes et chercheurs sur le génome humain) font face à des dangers particulièrement subtiles.

Note sur la structure des dossiers

Il y a fondamentalement deux manières d'organiser les dossiers médicaux électroniques. La première reflète le système papier existant ; chaque médecin conserve des dossiers dans son propre ordinateur (ou son fichier manuel), et l'information circule entre eux sous forme de notes succinctes. La seconde suppose que, pour chaque patient, il y a un dossier électronique unique, ouvert à sa naissance et fermé à sa mort, dans lequel seront inscrites toutes les informations d'intérêt médical.

Dans ce qui suit, nous commencerons par utiliser le premier modèle, car c'est celui qui prévaut aujourd'hui et car il est beaucoup plus simple. Après avoir développé une politique de sécurité dans ce cas, nous envisagerons la seconde approche, qui, bien que ce ne soit pas nécessaire, se traduira certainement par la création d'une base de données centralisée. Enfin, nous chercherons un compromis permettant, non seulement de garder les dossiers détaillés sur les ordinateurs des médecins, mais encore d'avoir un récapitulatif centralisé contenant des liens vers eux.

3.1 Contrôles d'accès

Dans une système informatisé, chaque sujet a accès à certains objets. L'information définissant cet accès peut être enregistrée par sujet ou par objet. Dans le premier cas, la permission d'accès est appelée capacité ou faculté et peut avoir la forme : « le Docteur Jones peut lire les dossiers de Farid Abdullahi, James Adams, Wendy Adams, Henry Addenbrookes, … » Si les permissions sont enregistrées par objet, on parle de liste de contrôle

d'accès qui peut avoir la forme : « ceci est le dossier de Farid Abdullahi et il peut être lu par le Docteur Jones, le Docteur Smith et l'infirmière Young. » Cette dernière approche conduit à une conception plus simple, étant donné que le nombre de patients par docteurs est beaucoup plus grand que le nombre de docteurs par patient.

Dans le cours normal des choses, tout médecin ayant accès à un dossier peut non seulement le lire, mais aussi y ajouter des informations (nous parlerons de la suppression d'informations dans un autre paragraphe). Notre premier principe est donc le suivant :

> **Principe 1 :** Chaque dossier médical identifiable devrait être marqué avec une liste de contrôle d'accès désignant les personnes ou groupes de personnes qui peuvent le lire et y ajouter des informations. Le système devrait empêcher toute personne ne figurant pas sur cette liste, d'accéder à ce dossier, par quelque moyen que ce soit.

Dans beaucoup de systèmes actuels, ces listes de contrôle d'accès sont implicites. Si un dossier est présent dans la base de données d'un centre médical, alors tous les médecins de ce centre peuvent le lire et le compléter. Cependant, avec l'introduction d'un réseau informatique, les listes de contrôle d'accès doivent être rendues explicites et consistantes à travers les différents systèmes ; elles doivent être imposées par des mécanismes efficaces techniquement, mais supportant des pratiques comme le travail intérimaire et le partage de dossiers.

L'utilisation de groupes d'utilisateurs permet de faciliter ceci. Par exemple, si le Docteur Jones, le Docteur Smith et l'infirmière Young font partie de la même équipe ou du même centre médical, appelé par exemple Swaffham, alors les dossiers auxquels ils ont tous trois accès pourraient simplement porter la mention « Swaffham. » Cette idée est inhérente au développement de la communauté médicale ; les équipes sont constituées de médecins, d'infirmières et d'employés des services sociaux, et le consentement écrit du patient pour partager les information est obtenu lors de la première prise de contact. De cette façon, les patients savent à qui accorder leur confiance.

Pourtant, dans certains cas, les seuls groupes pouvant être utilisés impliquent un grand nombre de personnes. Dans les grands hôpitaux par exemple, des centaines d'infirmières peuvent être assignées dans un service particulier. Des restrictions supplémentaires sont alors nécessaires pour définir les groupes ; un groupe peut alors prendre la forme « tout personnel médical travaillant dans l'unité où est soigné le patient. » Une telle approche serait l'équivalent électronique de la traditionnelle feuille de soins accompagnant le patient, mais avec l'avantage qu'un enregistrement de « qui a consulté quoi » peut être conservé.

À chaque fois que des groupes sont utilisés — qu'il s'agisse de groupes simples de quelques personnes, ou d'autres plus complexes avec des emplacements et d'autres contraintes — un enregistrement de toutes les consultations ou mises à jour du dossier correspondant doit toujours être gardé. Les groupes ne sont pas des médecins virtuels, mais des mécanismes simplifiant la correspondance entre accès, médecin et patient. Les concepteurs des systèmes informatisés devraient garder à l'esprit qu'un utilisateur donné peut très bien appartenir à différents groupes : il peut être à la fois, patient, médecin, enseignant, étudiant, directeur ou consultant auprès des autorités sanitaires. À moins que des mesures ne soient prises pour prendre en compte cette complexité, il est peut probable que cela se passe bien ; les méthodes au cas par cas devraient être évitées.

Il n'est pas acceptable, par exemple, qu'un groupe se résume en fait à un mot de passe partagé entre les membres d'une équipe, ou à un terminal « loggué » en permanence. De tels abus impliquent que les fautes ne peuvent plus être attribuées à un individu particulier, ce qui, dans certains cas, peut avoir des conséquences dangereuses, comme par exemple, le cas de ce patient psychopathe qui a utilisé le terminal d'uns équipe de soins afin de modifier une ordonnance dans un but meurtrier.

Lorsqu'un patient ouvre un dossier dans un cabinet médical ou au début une hospitalisation, il doit être informé des pratiques en matière de contrôle d'accès. Il doit avoir l'opportunité de les refuser et de limiter l'accès à quelques médecins de son choix. Pour cette raison, les systèmes basés sur les fonctions des utilisateurs doivent aussi prendre en compte des listes de contrôle d'accès encore plus restrictives, et notamment celles contenant seulement le nom d'un médecin (plus, bien sûr, celui du patient).

Une telle liste pourrait même être la liste par défaut dans le cas de données très sensibles. Le patient est seul juge du niveau de sensibilité des informations le concernant. De prime abord, sont très sensibles : les dossiers psychiatriques, les informations concernant des maladies sexuellement transmissibles et toutes les informations concernant des tiers (se référer à [GC95] p.44 pour une liste plus complète). Un militant pour le SIDA pourra peut-être demander à rendre sa séro-positivité publique, alors qu'un témoin de Jéhovah aura honte de parler d'une simple transfusion sanguine.

Finalement, il existe un grand nombre d'utilisateurs, comme les contrôleurs et les chercheurs, qui n'ont aucun accès en écriture aux dossiers. Nous développons ce cas dans un autre paragraphe, mais nous n'apporterons pas de clause particulière dans cette politique. Nous considérerons plutôt que ces personnes ont un accès complet (lecture, modification) à une copie temporaire des dossiers ; et c'est en fait un meilleur modèle de la réalité.

3.2 Ouverture d'un dossier

Au lieu d'utiliser des objets avec plusieurs listes de contrôle d'accès, nous préférons avoir plusieurs sous-dossiers par patient, par exemple :

- Un dossier principal ouvert à tous les médecins d'une équipe ;
- Un dossier très sensible pour le traitement d'une dépression, ouvert uniquement pour le médecin habituel ;
- Un dossier sur ses problèmes cardiaques ouvert à tout le personnel en charge des blessés et dont une copie pourrait être conservée dans une carte médicale d'urgence portée en permanence par le patient.

Un médecin pourrait alors ouvrir un nouveau sous-dossier lorsqu'un de ses patients désire lui parler d'un problème très privé, ou lorsqu'un nouveau patient le consulte, ou encore lorsqu'un patient est transféré depuis un autre hôpital. La liste de contrôle d'accès sur un nouveau dossier se présente comme suit :

> **Principe 2 :** Un médecin peu ouvrir un dossier avec son nom et celui du patient sur la liste de contrôle d'accès. Lorsqu'un patient a été transféré, il peut ajouter à cette liste le ou les médecins déjà en charge du patient.

3.3 Contrôle

À part le patient lui-même, seulement du personnel soignant peut avoir accès des informations personnelles sur sa santé. La raison de cette limitation est à la foi traditionnelle et pratique : les personnels soignants ne considèrent pas que les lois civiles et criminelles soient des protections adéquates. Si un médecin donne un dossier à un employé des services sociaux qui le passe ensuite à un tiers sans consentement — ou le conserve simplement dans une endroit peu sûr — alors le médecin pourrait être tenu responsable, sans recours possible.

En fait seuls les médecins peuvent garantir le principe de consentement et le contrôle des dossiers médicaux identifiables doit rester entre les mains du médecin responsable. Cela peut être le médecin généraliste du patient ou le médecin responsable d'une unité de soins dans un hôpital :

> **Principe 3 :** L'un des médecins de la liste de contrôle d'accès doit être désigné comme personne responsable. Seulement lui peut modifier la liste de contrôle d'accès en y ajoutant des professionnels soignant uniquement.

Dans les cas où l'accès a été octroyé aux administrateurs, comme aux États-Unis, le résultat a été l'abus. En Grande Bretagne, les tensions entre confidentialité médicale et « besoin de savoir » de l'Administration

ont été apaisées en instaurant au sein des organisation demandeuses des « zones franches » — espaces protégés sous le contrôle d'un médecin indépendant — dans lesquelles sont envoyées des copies de dossiers faisant l'objet de contestations administratives [NHS92]. Les systèmes administratifs devant manier des informations privées doivent supporter une telle procédure ; la partie médicale d'un dossier pourrait être chiffrée de telle façon que seul le médecin en charge de cette zone franche puisse la déchiffrer. De tels systèmes doivent aussi se conformer aux directives mentionnées dans [JCG88].

Quand un tiers (avocat, Police, compagnie d'assurance, employeur) réclame une information qui peut lui être transmise légalement, alors cette information doit lui être fournie sous forme papier. Cela reflète la pratique courante : les dossiers communs aux médecins, infirmiers et services sociaux sont conservés sur papier plutôt que dans des bases de données pour des raisons de sécurité.

Enfin il est bon de noter que des dossiers informatisés ne peuvent pas être utilisés comme preuve, à moins qu'ils ne soient accompagnés d'un certificat signé par le propriétaire ou l'opérateur du système.

3.4 Consentement et notification

Le patient doit donner son consentement pour toute modification de la liste de contrôle d'accès et doit être averti de tout ajout. En pratique, une notice, affichée dans le cabinet médical ou à la réception de l'hôpital, pourrait avertir que le médecin traitant ainsi que ses collègues immédiats seront automatiquement ajoutés sur cette liste, à moins que le patient ne s'y oppose. Dans tous les autres cas, comme, par exemple, le transfert vers un autre hôpital, l'avis du patient est nécessaire.

En revanche, lorsque des informations sont partagées en l'absence de consentement du patient, ce qui arrive en cas d'urgence après un accident, une lettre expliquant ce qui s'est passé doit être envoyée au patient. Il appartient au médecin qui a fourni l'information de le faire ; celui-ci serait vraiment très négligent s'il partait du principe que l'hôpital s'en chargera. Souvent, des personnes souhaitant se procurer illégalement des renseignements prétendent (par téléphone) être une infirmière travaillant dans un service d'urgence. Des conseils concernant la conception des procédures d'urgences sont données dans [And96] ; ce document insiste particulièrement sur la nécessité d'identifier la personne qui appelle (en la rappelant à un numéro référencé dans un registre officiel) et d'avertir le patient.

Cette notification est indispensable puisqu'elle permet de détecter des fraudes plus subtiles : corruption de personnel médical, utilisation du

budget d'autres patients lorsque des quotas sont imposés dans une unité de soins. Elle découle du principe de consentement.

Il n'y a pas d'exception à cette règle. Même lorsque qu'un médecin a légalement le devoir de passer une information à un tiers, le patient doit être averti. Dans certains cas très particuliers (abus d'enfants par exemple) la notification peut être retardée mais jamais annulée :

> **Principe 4 :** Le médecin responsable doit informer le patient des noms figurant sur la liste de contrôle d'accès de son dossier à sa création, après toute modification et à chaque fois que la responsabilité est transférée. Le consentement du malade doit être obtenu, sauf dans le cas d'urgences et dans le cas d'exemptions imposées par la loi.

Se pose aussi la question de la fréquence des notifications. Selon l'avis des médecins que nous avons consultés, une lettre annuelle est suffisante, à moins que des activités suspectes aient été détectées. Mais la question n'est pas si simple. Il y a peu de temps on a demandé aux médecins généralistes d'avertir les femmes utilisant certain moyens de contraception ; comment doit-on faire avec les jeunes filles prenant la pilule sans que leurs parents ne le sachent ou les femmes dont le conjoint a subi un vasectomie et qui continuent à prendre la pilule pour leurs relations extra-conjugales [Gil95] ? La solution, déjà pratiquée dans les cliniques spécialisées dans les maladies sexuellement transmissibles, est simplement de demander au patient comment doivent être envoyées ces notices.

Enfin, il faut mettre en place des procédures permettant de traiter efficacement les plaintes afin que les malfaiteurs soient punis : licenciements, actions disciplinaires, poursuites en justice. Que doit faire un patient lorsque, sur sa lettre annuelle, figure le nom d'une personne qu'il n'a jamais consultée ? Se rendre chez son médecin, en faire part au General Medical Council, à la Police, à la Presse ? La solution à ce problème dépend du succès du projet de loi déposé par la British Medical Association qui permettrait d'enchâsser la confidentialité de l'information personnelle de santé dans les textes de loi [BMA95].

3.5 Persistance

Il existe des règles concernant la durée pendant laquelle doivent être conservés les dossiers médicaux. La plupart des dossiers principaux doivent être gardés huit ans, ceux relatifs à un cancer pendant toute la vie du patient et ceux décrivant une maladie génétique encore plus longtemps. Dans chaque cas, la prudence impose de garder ces dossiers tant qu'un procès pour négligence professionnelle peut être intenté. Le principe suivant est donc simple :

Principe 5 : Personne ne doit pouvoir effacer un dossier médical avant que sa date d'expiration appropriée ait été atteinte.

Toutefois, cette règle n'est pas encore toujours suivie, et l'utilisation du mot « approprié » couvre un certain nombre de questions importantes :

- Notre formulation permet la destruction de vieux dossiers mais ne l'impose pas ; il y a beaucoup de cas (comme les maladies chroniques) dans lesquels il est approprié de garder des dossiers pour une durée supérieure à celle réclamée par la loi ;
- Le sixième principe de la loi sur la protection des données (Data Protection Act [DPA84]) stipule que les informations « ne devraient être gardées plus longtemps que nécessaire. » Cela signifie qu'à partir du moment ou un médecin n'est plus le détenteur principal d'un dossier (par exemple si le patient déménage), alors ce dernier doit être détruit. Cependant il serait souhaitable que ce dossier puisse être disponible si nécessaire (par exemple lors d'un procès) ;
- Le consentement du patient n'est pas immuable, mais est plutôt un dialogue constant entre lui et son médecin [Som93]. Il est donc tout à fait possible qu'un patient retire son consentement et insiste pour que le dossier soit détruit. Aucun cas de justice ne nous a été relaté ; la solution pourrait probablement être le transfert du dossier primaire chez un médecin choisi par le patient jusqu'à la fin de la période réglementaire ;
- La durée de vie appropriée des copies temporaires est plus courte. Cela concerne les copies maintenues dans des zones franches (cf. paragraphe 3.1), ou celles utilisées par des contrôleurs ou des chercheurs ; par exemple, l'autorisation pour échanger des dossiers avec des chercheurs doit être renouvelée tous les cinq ans [Som93], par conséquent toute copie détenue par des chercheurs ne devrait pas persister plus longtemps et devrait normalement être détruite bien avant. La conception et la mise en application de ces impératifs ont un impact direct sur le contrôle de l'agrégation, dont il est question ci-après.

La conservation des dossiers n'est pas aussi simple qu'on pourrait le penser ; il ne faut pas que des informations inexactes qui ont été détectées (erreurs simples, ou diagnostiques révisés) conduisent ultérieurement à des erreurs lors du traitement. En revanche il ne faut pas faciliter la suppression sans trace des fautes, puisque cela ferait perdre au dossier sa valeur de preuve. Par conséquent (et comme dans beaucoup de systèmes financiers ou comptables), l'information devrait être mise à jour en ajoutant plutôt qu'en effaçant, la version la plus récente devant retenir l'attention du médecin. L'effacement devrait être réservé pour les dossiers ayant atteint leur date d'expiration.

Une formulation équivalente du principe ci-dessus peut être trouvée dans les exigences actuelles permettant d'accréditer les systèmes informatisés des médecins généralistes et stipulant que « le système ne doit pas permettre l'altération ou l'effacement des dossiers à moins qu'un mécanisme sûr puisse permettre de les reconstruire tels qu'ils étaient à n'importe quelle date dans le passé » [RFA93].

3.6 Imputation

Nous devons maintenant nous assurer que tous les accès aux dossiers médicaux (que ce soit lecture, ajout ou effacement) puissent être attribués correctement à quelqu'un :

> **Principe 6 :** Tous les accès à des dossiers médicaux doivent être consignés avec le nom du sujet la date et l'heure. Une trace de tous les effacements, doit aussi être gardée.

Les systèmes tenant compte de cette exigence doivent typiquement enregistrer tous les accès en écriture. Même si des données sont supprimées du dossier principal, il existe un journal qui permet de le restaurer dans l'état où il était à un instant donné et d'imputer les changements à leurs auteurs respectifs [RFA93]. Les accès en lecture doivent être consignés, afin de punir les abus de confiance ; les suppressions doivent également être consignées, afin que les personnes ayant délibérément détruit des informations compromettantes puissent être retrouvées.

Certaine applications ont des exigences très rigoureuses en matière d'imputation. Par exemple une notice de non réanimation sur le dossier d'un patient hospitalisé doit être signée par le chirurgien consultant en charge et requiert le consentement du patient, si celui-ci est capable de le donner [Som93]. Quand des fonctions aussi critiques sont automatisées, les mécanismes — y compris ceux d'imputation — doivent être construits avec autant de soins et avec les mêmes standards que les systèmes permettant de maintenir un malade en vie.

Enfin, il existe des exigences d'imputation qui sont rarement évoquées. À quelques exceptions près les patients peuvent lire leurs dossiers médicaux et peuvent y apporter des objections. Ces requêtes sont rares, et sont donc habituellement traitées sur papier : le médecin imprime les dossiers que le patient souhaite consulter, apporte éventuellement les corrections nécessaires et remet au patient une copie de la nouvelle version pour confirmation. Nous n'avons aucune objection contre ces procédures. Nous n'imposons pas une sécurité entièrement logicielle ; nous nous intéressons aux effets du traitement à la foi manuel et automatisé.

3.7 Flux de l'information

Le seul flux d'information possible entre deux dossiers d'un même patient avec des listes de contrôle d'accès différentes va du dossier le moins sensible vers les plus sensible :

> **Principe 7 :** Une information issue du dossier A peut être ajoutée au dossier B si et seulement si la liste de contrôle d'accès de B contient celle de A.

Les mécanismes techniques requis pour appliquer un tel principe sont décris dans des livres de sécurité informatique de base tel Amoroso [Amo94] : la liste de contrôle d'accès d'un processus doit être réduite à l'intersection des listes de contrôle d'accès des dossiers qu'il a lus, et ce processus ne doit pouvoir écrire que dans un dossier dont la liste de contrôle d'accès est incluse dans la sienne.

Lorsque deux dossiers avec des listes de contrôle d'accès différentes correspondent au même patient, la question difficile est de savoir si l'existence même du dossier sensible sera indiquée dans l'autre. C'est l'un des perpétuels dilemmes pour lesquels il n'y a pas encore unanimité [GC95]. S'il existe des informations dissimulées, que ce soit explicitement ou par l'absence notable de certain enregistrements, alors des conclusions peuvent en être tirées. Dans les Pays-Bas, par exemple, les médecins retiraient systématiquement du système informatique les dossiers des patients atteints d'un cancer. Le résultat a été immédiat : lorsque que les assureurs et les fonds de pension constataient l'absence d'un dossier, il savaient avec une forte probabilité que le sujet souffrait du cancer [Cae95].

En l'absence d'indications d'autres problèmes surviennent. Supposons en effet que le patient d'un psychiatre demande à faire un test de dépistage du SIDA et exige que le résultat soit tenu secret. Avant que le résultat ne soit connu et suite au stress le patient fait une rechute qui conduit le psychiatre à ne plus le considérer comme compétent pour avoir accès à son dossier médical. N'étant pas au courant du test demandé par le patient, le psychiatre ne signale pas le nouveau statut du patient au centre de dépistage. Il n'est pas possible de résoudre ce problème en créant un registre des personnes incapables, puisque les troubles cérébraux sont confidentiels et dépendent des circonstances. Une autre conséquence de la non-indication des dossiers sensibles est que les personnes souffrant du syndrome de Munchhausen sont plus difficiles à détecter et à gérer.

Nous pensons que les médecins opterons pour des annotations discrètes indiquant seulement la présence d'informations cachées ou à accès restreint. Cela suggéra au médecin de demander après qu'une certaine relation de confiance a été établie : « y a-t-il autre chose que vous pourriez me dire et qui pourrait être pertinent ? ».

Dans tous les cas, les concepteurs de systèmes informatisés devraient apporter une attention particulière à la propagation des attributs sensibles à travers différents dossiers et à ses effets sur l'intégrité du système.

Finalement, des mécanismes permettant de publier des données rendues anonymes sont nécessaires. Comme pour le déclassement de l'information dans les systèmes à plusieurs niveaux de sécurité, nous n'incorporerons pas ceux-ci dans la politique de sécurité. Nous recommandons cependant d'exiger un acte délibéré du médecin et consigné dans un registre avant de publier un dossier considéré comme anonyme.

3.8 Contrôle de l'agrégation

L'utilisation de listes de contrôle d'accès et de lettres de notification envoyées aux patients est utile contre les menaces d'agrégation mais n'est pas suffisante pour les en empêcher. Le médecin en charge d'une zone franche (cf. paragraphe 3.1) peut être ajouté sur les listes de contrôle d'accès de millions de patients hospitalisés, le rendant vulnérable aux incitations ou aux menaces de trafiquants de données.

> **Principe 8 :** Des mesures efficaces empêchant l'agrégation des informations personnelles de santé doivent être mises en place. En particulier, les patients doivent recevoir des notifications spéciales si une personne ayant déjà accès aux dossiers d'un grand nombre de personnes doit être ajoutée sur leur liste de contrôle d'accès.

Certains systèmes informatiques d'hôpitaux existants, accumulent des informations privées sur un million de patients ou plus ; l'ensemble des utilisateurs de ces systèmes ont accès à ces informations. À présent, le contrôle typique est une déclaration selon laquelle tout accès injustifié sera passible de licenciement ; mais la mise en vigueur de ces règles est sporadique et des incidents similaires au cas Jackson continuent d'être reportés. En général, les systèmes des centres hospitaliers sont mal administrés [AC95a] [AC95b].

Les systèmes hospitaliers accordant l'accès à tous les dossiers médicaux par tout le personnel soignant ne doivent pas être connectés aux réseaux informatiques. Avoir 2 000 employés pouvant consulter un million de dossiers est déjà une mauvaise chose ; mais la perspective de 200 hôpitaux similaires, permettant à 400 000 employés de consulter les dossiers de l'ensemble de la population est inadmissible.

Il existe des applications pour lesquelles l'agrégation des données est inévitable, c'est le cas notamment des programmes de vaccination des enfants. Les systèmes devant les traiter devront être conçus intelligemment.

Comme indiqué ci-dessus, les dossiers peuvent être agrégés, à condition qu'ils soient rendus suffisamment anonymes. Il a été suggéré que cette condition pouvait être remplie en remplaçant le nom des patients par leur numéro de sécurité sociale et les diagnostiques par des codes [RSM92]. Un certains nombre de systèmes ont d'ailleurs été conçus partant du principe que cette solution était satisfaisante ; ce n'est pas le cas.

Rendre les données anonymes est difficile surtout si ces données peuvent être croisées avec d'autres : si une personne mal intentionnée peut interroger la base de données avec des requêtes du type « montre moi les dossiers de toutes les femmes de 35 ans, avec deux filles de 13 et 15 ans souffrant toutes deux d'eczéma, » alors elle peut identifier les individus. Les limitations au croisement de données, et les techniques pour empêcher l'inférence ont été étudiées minutieusement dans le contexte du recensement de la population. Quand les recherches sont purement statistiques, ces méthodes peuvent être utilisées ; quand ce n'est pas le cas il pourrait être accordé aux chercheurs un accès aux données mais dans un espace protégé.

3.9 La base informatique de confiance

Enfin nous devons nous assurer que les mécanismes de sécurité sont efficaces en pratique comme en théorie. Cela conduit aux questions d'évaluation et d'accréditation. La base informatique à qui l'on se fier, est l'ensemble du matériel, des logiciels et des procédures qui permettent d'appliquer efficacement la politique de sécurité. Cela signifie que pour contourner ces mesures de sécurité, un attaquant doit subvertir l'un de ces composants.

À ce stade, nous souhaitons clarifier ce que nous entendons par « faire confiance. » Dans le langage courant, quand nous disons que nous faisons confiance à une personne, nous nous en remettons à elle pour faire — ou ne pas faire — certaines choses. Par exemple, un patient confiant des informations à son médecin espère que ce dernier ne les divulguera pas à des tiers sans son consentement et que ses attentes ne seront pas déçues.

Une autre façon de regarder cette relation a déjà été employée avec succès dans la conception des systèmes informatisés : une personne de confiance est une personne pouvant contourner les mesures de sécurité. Ainsi un médecin en possession d'informations confidentielles sur ses patients peut leur causer du tort révélant ces informations ; cela ne dépend que de lui. Il existera des composant du système informatisé dont nous dépendrons de la même manière. S'ils sont subvertis, ou s'ils contiennent des erreurs, alors la politique de sécurité peut être contournée.

La base informatique de confiance peut inclure des mécanismes de sécurité du traitement pour appliquer l'authentification des utilisateurs et le contrôle des accès, des mécanismes de sécurité de communication afin de réduire les accès aux informations en transit sur un réseau de télécommunication, des mesures statistiques pour s'assurer que les chercheurs et contrôleurs n'ont pas suffisamment de données en leur possession pour identifier les patients et enfin des mécanismes de disponibilité comme les sauvegardes systématiques garantissant la restauration des données en cas de perte ou de vol.

Il n'est pas suffisant de se contenter des assurances du fournisseur selon lesquels son matériel est sûr — ces affirmations doivent être vérifiées par un tiers compétent et indépendant.

> **Principe 9 :** Les systèmes informatiques utilisés dans le domaine de la Santé doivent comporter des sous-systèmes imposant de manière efficace les principes développés précédemment. Cette efficacité doit être contrôlée par des experts indépendants.

L'expérience prouve que l'évaluation est nécessaire ; il existe maintenant un schéma européen, ITSEC [EU91], suivant lequel les agences nationales de sécurité informatique permettent à des laboratoires commerciaux indépendants d'évaluer leur sécurité. Une accréditation par un organisme indépendant est aussi de rigueur dans d'autres pays : Australie [Aus95], Canada [TCP93], et États-Unis [TCS85]. Étant donné que des schémas, comme ITSEC, sont plutôt destinés à des systèmes militaires et qu'une évaluation en suivant leurs recommandations peut être très coûteuse, certaines entreprises proposent leur propre schéma d'évaluation. Par exemple, la sécurité des alarmes contre les cambriolages est contrôlée par des laboratoires mandatés par le Loss Prevention Council de Grande Bretagne. Des contrats similaires pourraient être établis dans le domaine de l'informatique médicale.

3.10 Dossiers médicaux ou dossiers sur les patients

Comme nous avons pu le noter précédemment, la plupart des systèmes informatiques médicaux reflètent la pratique courante en ce sens que chaque équipe de soins conserve des dossiers, et que l'information passe d'équipe en équipe sous forme de résumés (lettres de décharge, avis, résultats de laboratoire, etc.). Un dossier entier peut être copié pour une autre équipe si le patient est transféré, mais, en général, les dossiers sont établis sur la base des médecins plutôt que des patients.

Une certaine attention a été portée vers un autre modèle, un « dossier électronique unifié par patient, » qui accumule toutes les notes médicales colligées au cours de la vie du patient [MRI94]. Mais sécuriser un dossier unifié est compliqué, et ce, pour plusieurs raisons:

- Si l'information est enregistrée sur une carte optique ou une disquette en possession du patient, comment la récupère-t-on en cas de perte ? Mais alors si des sauvegardes sont faites dans une base de données centralisée comment contrôle-t-on l'agrégation ?
- Les enregistrements de naissance contiennent également des informations personnelles sur la santé de la mère. Le patient y aura-t-il accès ?
- Que doit-on faire des fichiers de grande taille tels que les images obtenues par tomographie assistée par ordinateur ou les enregistrements relatifs à une longue maladie chronique ?
- Comment garantir aux médecins la possibilité d'accéder à des dossiers d'anciens patients afin d'évaluer les soins qu'ils leur ont prodigués et de se défendre en justice ?
- Est-ce que des dossiers ordonnés suivant les patients nous obligent à identifier avec soins celui-ci, et si c'est le cas, quelles sont les implications quand des soins d'urgence doivent être donnés ou quand le patient demande à être traité anonymement (telle une jeune fille de quatorze ans souhaitant avorter).
- Le fait qu'un patient reçoive des soins en prison, ne peut être inscrit ailleurs que dans le dossier carcéral, qui, de façon réaliste, ne peut être conservé en dehors de la prison pas plus qu'un dossier particulièrement sensible ne peut être entre les mains d'un seul médecin. Quel est l'intérêt d'un système centralisé si des fichiers locaux doivent subsister ?

La liste précédente est loin d'être exhaustive. Une discussion plus avancée sur les complexités des systèmes traitant des dossiers organisés par patient est proposée dans [GC95]. Clairement, l'utilisation de dossiers électroniques unifiés pour chaque patient nous obligerait à ajouter un certain nombre de principes à notre politique.

Des systèmes hybrides existent. Plutôt que de rassembler l'ensemble des informations concernant un patient dans un seul fichier, l'idée est de créer une sorte de table des matières centrale comportant des liens vers les fichiers conservés par les médecins. Au moins deux hôpitaux Britanniques essayent des méthodes basées sur ce modèle.

5 Conclusions

Nous avons décrit ce qui pouvait menacer la confidentialité, l'intégrité et la disponibilité des systèmes d'informations dans le domaine de la Santé, et ce, à la lumière de l'expérience de la Grande Bretagne et de pays

étrangers. Nous avons proposé une politique de sécurité pour l'information médicale qui permet de faire appliquer le principe de consentement du patient notamment dans les systèmes distribués hétérogènes en construction en Grande Bretagne.

Nous encourageons les médecins donnant leur avis sur les matériels à acheter à favoriser les systèmes suivant cette politique. Lorsqu'aucun système compatible n'est disponible, ces médecins devraient s'informer dans quelles mesures les principes exposés ici sont respectés et si le fabricant entend fournir par la suite des mises à jours permettant de rendre le système compatible.

Si aucun des systèmes disponibles sur le marché n'offre un niveau acceptable de sécurité, la British Medical Association avise ses membres que l'exposition de dossiers médicaux identifiables et non protégés sur le réseau du National Health Service (et, en fait, sur n'importe quel réseau), est imprudente voire en contradiction avec la déontologie — même si ces dossiers sont envoyés de façon chiffrée vers un système peu fiable.

Remerciements : Nous tenons à remercier les professionnels de Santé, informaticiens et philosophes qui, par leurs avis éclairés, ont contribué à la rédaction de ce document et notamment :

- Professionnels de Santé : Fleur Fisher, Tony Griew, Simon Jenkins, Grant Kelly, Stuart Horner, Hilary Curtis, Simon Fradd, John Williams, Iain Anderson, William Anderson, Roger Sewell, Mary Hawking, Ian Purves, Paul Steventon, Steve Hajioff, Stan Shepherd, Jeremy Wright and David Watts;
- Informaticiens : Stewart Lee, Roger Needham, Mark Lomas, Bruce Christianson, Ian Jackson, Mike Roe, Jeremy Thorp, Roy Dainty and Ian Keith;
- Philosophes : Beverly Woodward, Ann Somerville and Keith Tayler.

Biographie : Ross J. Anderson a obtenu son titre de Docteur à l'Université de Cambridge où il est aujourd'hui chercheur et enseignant. Fort de sa longue expérience dans les domaines de la sécurité informatique et de la cryptographie, plusieurs foi récompensé, il conseille la *British Medical Association* sur les problèmes liés à l'informatisation.

Bibliographie

[ACH95] *Keeping Information Confidential*, Association of Community Health Councils for England and Wales, mai 1995

[RAC93] *Interim Code of Practice for Computerised Medical Records in General Practice*, Royal Australian College of General Practitioners, février 1993

[BMA95] *A Bill Governing Collection, Use and Disclosure of Personal Health Information*, British Medical Association, 1995

[Som93] *Medical Ethics Today — Its Practice and Philosophy*, A. Sommerville, British Medical Association, 1993

[EU95] *On the protection of individuals with regard to the processing of personal data and on the free movement of such data* (final), Directive du Parlement Européen du Conseil, adoptée par le Conseil le 24 juillet 1995

[GMC1] *Good medical practice*, General Medical Council, 178–202 Great Portland Street, London W1N 6JE

[GMC2] *Confidentiality*, General Medical Council, 178–202 Great Portland Street, London W1N 6JE

[DGMW94] *How to Keep a Clinical Confidence*, B. Darley, A. Griew, K. MsLoughlin, J. Williams, HMSO,[2] 1994

[Mac94] Lettre de A.W. Macara à J.S. Metters concernant *Draft guidance for the NHS on the confidentiality, use and disclosure of personal health information*, 31 octobre 1994

[LB94] *Your Secrets for Sale*, N. Luck, J. Burns, The Daily Express, 16 février 1994, pp.32–33

[Smu94] *Health Care Information: Access and Protection*, R.H. Smuckler, Institute for Primary Care Informatics, 1994

[RL95] *For Sale: your secret medical records for 150 pounds*, L. Rogers, D. Leppard, Sunday Times, 26 novembre 1995, pp.1–2

[JHC94] *Nurse Jailed for Hacking into Computerised Prescription System*, British Journal of Healthcare Computing and Information Management vol.1, 1994, p.7

[Tho95] *Sex Stalker Plays Doctor to Trick Victims*, M. Thomas, PA newswire no 1236, 7 juillet 1995

[GTP93] *Privacy and Security of Personal Information in a New Health Care System*, L.O. Gostin, J. Turek-Brezina, M. Powers *et al.*, Journal of the American Medical Association, vol.20, 24 novembre 1993, pp.2487–2493

[CR94] *Who's reading your medical records?*, Consumer Reports, octobre 1994, pp.628–632

[Bru95] *Is your health history anyone's business?*, McCall's Magazine, avril 1995, p.54, rapporté par M. Bruce sur Usenet news-group `comp.society.privacy`, 22 mars 1995

[HRM93] *RMs need to safeguard computerised patient records to protect hospitals*, Hospital Risk Management, vol.9, septembre 1993, pp.129–140

[See95] *Marketing use of medical DB*, M. Seecof, Usenet newsgroup `comp.risks`, ref.17.12

[OTA93] *Protecting Privacy in Computerized Medical Information*, Office of Technology Assessment, US Government Printing Office, 1993

[Woo95] *The computer-based patient record and confidentiality*, B. Woodward, New England Journal of Medicine vol.333 no.21, 1995, pp.1419–1422

[WHC95] Réunion de travaille sur le système de Santé et la confidentialité tenu à la British Medical Association le 4 avril 1995 ; transcription fournie par R.H. Pyne

[Haw95] *Confidentiality of personal information: a patient survey*, A Hawker, Journal of Informatics in Primary Care, mars 1995, pp.16–19

[Mar95] *Fear of Flowing*, D.C. Markwell, Proceedings of the 1995 Annual Conference of The Primary Health Care Specialist Group of the British Computer Society, pp.36–42

[Ald95] *Nurse sacked for altering records after baby's death*, K. Alderson, The Times, 29 novembre 95, p.6

[USA95] *Online medical records raise privacy fears*, USA Today, 22 mars 1995, pp.1A–2A

[DPR95] *Identity Cards: A Consultation Document CM2879 — Response of the Data Protection Registrar*, octobre 1995

[PK95] *GP Practice computer security survey*, R.A. Pitchford, S. Kay, Journal of Informatics in Primary Care, septembre 1995, pp.6–12

[NHS95] *The Handbook of Information Security — Information Security withinGeneral Practice*, NHS Executive Information Management Group E5209, mai 1995

[And96] *Medical System Security — Interim Guidelines*, R. Anderson, dans British Medical Journal vol.312 no.7023, 13 janvier 1996, pp.109–111

[AIS95] *AIS — Advanced Information System*, FHS Computer Unit, 1995

[DL95] Informations sur les produits de la société Data Logic disponibles à l'adresse : `http://www.datlog.co.uk/`

[JCG88] *GMSC and RCGP guidelines for the extraction and use of data from general practitioner computer systems by organisations external to the practice*, Annexe III dans *Committee on Standards of Data Extraction from General Practice Guidelines*, Joint Computer Group du GMSC et du RCGP, 1988

[GC95] *A Strategy for Security of the Electronic Patient Record*, A. Griew, R. Currell, Institute for Health Informatics, University of Wales, Aberystwyth, 14 mars1995

[NHS92] *Handling confidential patient information in contracting: A Code of Practice*, NHS Information Management Group EL(92)60, catalogue numéro 2009(c)

[Gil95] *MDU Muddle re Death Pills*, C. Gilbert, liste de distribution électronique « gp-uk », 23 octobre 1995

[DPA84] *Data Protection Act*, HMSO,[2] 1984

[RFA93] *Requirements for accreditation, general medical practice computer systems*, NHS Management Executive, 1993

[Amo94] *Fundamentals of Computer Security Technology*, E. Amoroso, Prentice Hall, 1994

[Cae95] W.J. Caelli, conversation privée, juillet 1995

[AC95a] *Setting the Records Straight — A Study of Hospital Medical Records*, Audit Commission, juin 1995

[AC95b] *For Your Information — A Study of Information Management and Systems in the Acute Hospital*, Audit Commission, juillet 1995

[RSM92] *Computers in Medical Audit*, dexième édition, M. Rigby, A. McBride, C. Shields, Royal Society of Medicine, London, 1992

[EU91] *Information Technology Security Evaluation Criteria*, document de la Communauté Européenne COM(90) 314, juin 1991

[Aus95] *Australian Standard 4400: Personal privacy protection in health care information systems*, Standards Australia, 1995

[TCP93] *The Canadian trusted Computer Product Evaluation Criteria*, Communications Security Establishment, Gouvernement Canadien, janvier 1993

[TCS85] *Trusted Computer System Evaluation Criteria*, Ministère de la Défense Américain, document 5200.28-STD, décembre 1985