Table des matières

Table des abréviations

Voici la liste alphabétique des abréviations et acronymes utilisés dans ce document :

ARRA : American Recovery and Reinvestment Act (USA)

ASIP Santé : Agence des Systèmes d'Informations Partagés de Santé (France)

DMP : Dossier Médical Personnel (France)

DSQ : Dossier Santé Québec

EIOM : Entrée Informatisée des Ordonnances Médicales

EHR : Electronic Health Record

ENAP : École Nationale d'Administration Publique

HAS : Haute Autorité de Santé (France)

HIA : Health Information Act (Alberta)

HISO : Health Information Standards Organisation (Nouvelle-Zélande)

HITECH Act : Health Information Technology for Economical and Clinical Health Act (USA)

HIPAA : Health Insurance Portability and Accountability Act (USA)

IOM : Institute of Medicine (USA)

MSSS : Ministère de la Santé et des Services Sociaux du Québec

PHI : Protected Health Information

PITO : Physician Information Technology Office (Colombie-Britannique)

PORA : Provincial Organizational Readiness Assessment (Alberta)

SIS : Systèmes Informatiques de Santé

Introduction

L'objet de ce rapport est de rendre compte des résultats d'une recherche effectuée au moment d'un stage au Ministère de la Santé et des Services Sociaux du Québec dans le cadre du programme de maitrise en administration publique de l'École Nationale d'Administration Publique.

Le mandat de stage porte sur les risques liés à l'informatisation de la santé.

La gestion de l'information n'est pas apparue avec l'avènement de l'informatique; les humains et les organisations gèrent des données et de l'information structurée depuis bien plus longtemps. Cependant, le monde de la gestion de l'information a connu un réel bouleversement avec l'informatisation. Jamais nous n'avons eu jusqu'à maintenant, un tel rapport à l'information, autant dans la diversité, dans le nombre d'échanges, ou dans la taille des stockages.

Et cette révolution touche tous les domaines, qu'il s'agisse des individus, de l'entreprise et même de la sphère publique. Aujourd'hui, en plus d'utiliser les nouvelles technologies de l'information et de la communication pour améliorer leur productivité et leur efficacité, les pouvoirs et services publics les intègrent également pour renouveler leur façon de rendre des services à la population ainsi que leurs relations avec la société civile. On constate aujourd'hui l'essor du vote électronique, du gouvernement «ouvert», en plus de l'offre croissante de services publics qui s'effectuent de plus en plus à l'aide d'Internet.

Le monde de la santé n'est pas ménagé par cette révolution de l'information, puisque de nombreuses données y sont utilisées, notamment dans le cadre des soins aux patients : historique de soins des patients, banques de données sur les médicaments, les pathologies et leur traitements, diagnostics, test et leurs résultats... Et tous ces renseignements sont d'une importance capitale pour que le traitement d'un patient soit le plus adéquat. Utiliser l'outil informatique pour gérer l'information de santé peut être un levier pour améliorer la qualité et la prestation des soins en rendant l'ensemble des renseignements nécessaires facilement accessibles e disponibles aux professionnels de la santé habilités. Parmi les bénéfices escomptés, l'informatisation de la santé vise l'augmentation d'efficacité des soins en favorisant le partage d'information tout en économisant du temps de gestion d'information.

Ainsi de nombreuses initiatives d'informatisation de la santé s'implantent un peu partout dans le monde, sous des formes diverses, amenées au nom de ces avantages potentiels. Pourtant, la preuve de gains d'efficacité ou de qualité des soins n'est souvent pas documentée ou

démontrée. Des changements d'une telle ampleur renouvèlent radicalement la manière dont on traite un patient et puisque l'état de santé voire la vie des patients ainsi que des investissements considérables sont en jeu, il est pertinent de se demander quels sont les changements apportés par l'informatisation et surtout ses impacts et conséquences potentielles. Puisqu'un changement technologique n'est jamais neutre, il est inévitable que des effets positifs et négatifs apparaissent. L'informatisation de la santé étant un phénomène récent, il est intéressant de vérifier les diverses approches retenues par les États pour gérer les risques issus de ces changements importants ainsi que leurs effets indésirables. En effet, il serait inquiétant que ces nouveaux outils informatiques soient mis en place en s'attardant uniquement sur les avantages pouvant être obtenus, et en escamotant les possibles inconvénients.

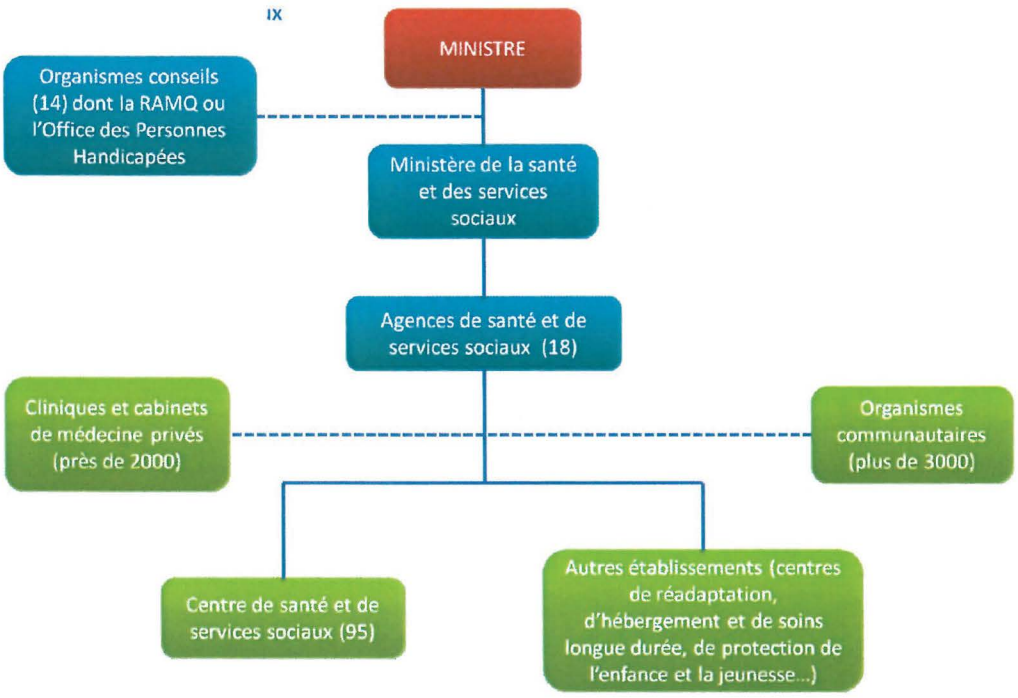
C'est dans ce sens que ce travail de recherche penche : il s'agit ici d'identifier quels sont les risques provoqués par l'informatisation de la santé, comment ils sont causés et quels dangers ils peuvent susciter (dans la partie contextualisation, recension des écrits). Pour ce faire, la situation de plusieurs pays (dans la première partie des résultats et ses annexes) sera étudiée afin de recenser les risques aujourd'hui reconnus et les mesures prises pour les contrer. Pour aller un peu plus loin, on s'intéressera aussi aux méthodes d'évaluation entourant ces mesures (dans la deuxième partie des résultats), dans un but d'amorcer une documentation des impacts de l'informatisation de la santé, sujet très peu exploré aujourd'hui.

Présentation de l'organisation et du mandat confié

1. Le Ministère de la Santé et des Services Sociaux

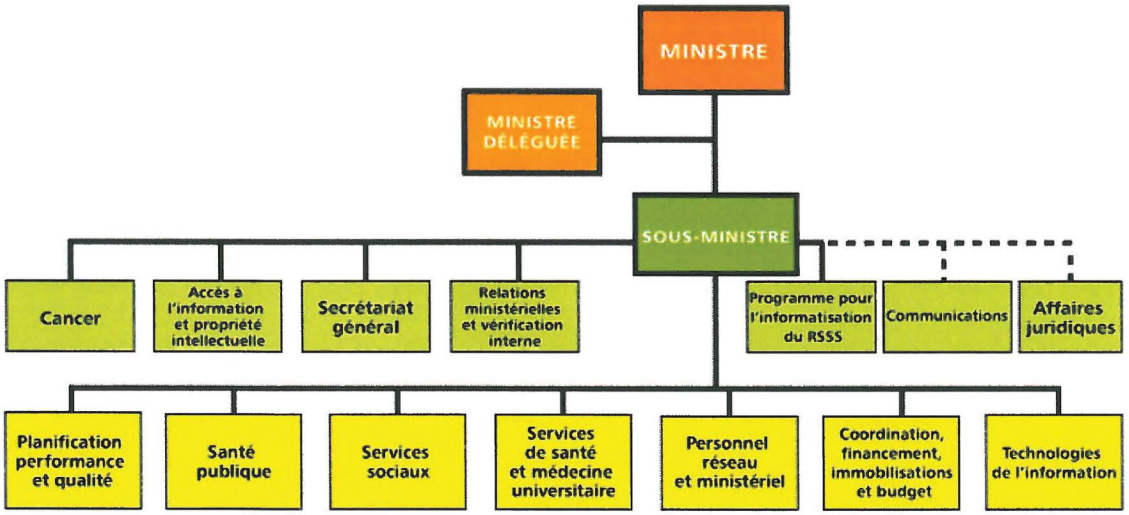
Le stage a été réalisé au Ministère de la Santé et des Services Sociaux du Québec, dont la mission, comme le prévoit la Loi sur les services de santé et les services sociaux est de « maintenir, d'améliorer et de restaurer la santé et le bien-être des Québécoises et des Québécois en rendant accessibles un ensemble de services de santé et de services sociaux, intégrés et de qualité, contribuant ainsi au développement social et économique du Québec ».

Le MSSS s'inscrit dans un système plus grand regroupant tous les acteurs de la santé et des services sociaux que l'on appelle le réseau de la santé et des services sociaux (RSSS). Le système Québécois a ceci de particulier que tous ces acteurs sont regroupés sous la même autorité. Il s'organise selon le schéma suivant :



Plus particulièrement, pour ce qui est de l'organisation du MSSS, sous la responsabilité du Ministre de la Santé et des Services Sociaux, du ministre délégué aux Services Sociaux et du Sous-ministre on trouve un certain nombre de directions et de services. On peut remarquer d'après son organigramme que le MSSS est responsable d'activités dans des champs de spécialisations très variés ce qui requiert de nombreuses compétences.

Figure 2 : Organigramme du MSSS en août 2012 (Source : Intranet du MSSS)



Les 7 directions générales que l'on voit sur le bas de l'organigramme, sont dirigées chacune par un sous-ministre adjoint et se décomposent encore en directions diverses. Le stage a été réalisé au sein de la direction générale des technologies de l'information, dans la direction de la sécurité des technologies de l'information.

2. La Direction de la Sécurité des Technologies de l'Information

La direction dans laquelle le stage a été effectué, fait partie de la direction générale des technologies de l'information. L'équipe qui compte environ une dizaine de personnes, est dirigée par Madame Sonia Roy, qui a été la directrice de stage pour la partie pratique. Les tâches incombant à cette direction sont multiples et se rapportent à de nombreux projets portés par le ministère dont le DSQ (Dossier Santé Québec), qui est en phase d'implantation.

3. Le mandat de stage

Le mandat du stage se compose de deux parties : tout d'abord une analyse comparative de plusieurs pays sur leurs réactions face aux risques posés par l'informatisation de la santé. L'autre partie, est quant à elle réservée à des perspectives d'évaluation de ce genre de mesures parce que du fait de la nouveauté de ces initiatives, on a encore peu de recul sur leur efficacité.

Au cours des rencontres préliminaires, ce mandat a été précisé pour arriver à une division en trois grandes tâches : une première partie du stage a été consacrée à des recherches générales sur le sujet de l'informatisation de la santé afin de pouvoir familiariser avec la problématique. Cela a aussi permis de dresser un inventaire des risques existants ainsi que de décider des pays qui seront retenus pour l'analyse comparative. Les deux autres parties correspondent aux deux champs de recherches proposés dans le mandat de stage.

4. Déroulement du stage

Les trois tâches ont été réalisées en séquences. Lors de la première partie, il s'agissait de s'entendre sur une définition des SIS et de l'environnement dans lequel ils agissent, ainsi que sur un ensemble de risques posés par l'introduction de ces dernier. Suite à cet inventaire, une recension des pays ayant implanté des SIS a été proposée afin de choisir les pays à étudier. Selon le temps imparti pour le stage, il a été convenu d'étudier le Québec et 3 autres provinces Canadiennes : l'Alberta, la Colombie-Britannique et l'Ontario. D'autre part, le Danemark, l'Estonie, les États-Unis, la France et la Nouvelle-Zélande ont été sélectionnés puisqu'ils reflètent assez bien la diversité des modes d'implantation et de réglementation des SIS à travers le monde.

La seconde partie du stage a été concentrée sur l'analyse comparative. Il s'agissait ici de trouver des informations fiables en provenance des pays sélectionnés et de réaliser des comparaisons entre les États.

La troisième partie du stage a été dévolue aux perspectives d'évaluation des mesures de sécurité prises par les États sur les SIS. Pour ce faire, il a fallu étudier autant les quelques travaux déjà publiés sur le sujet, qu'appliquer les connaissances issues des cours d'évaluation de programme à un cas pris comme exemple.

Contextualisation, recension des écrits

La littérature scientifique sur le sujet des SIS et surtout sur les nouveaux risques qu'ils entraînent n'est pas encore très fournie. Il s'agit d'un sujet récent et peu d'études chiffrées et où aucune typologie des risques qui soit reconnue, n'ont été réalisées. Dans cette partie, il s'agit plus de faire un regroupement de plusieurs notions qui apparaissent dans la littérature dans des modèles pertinents et efficaces pour la réalisation du mandat. Les modèles ne sont donc pas tirés directement de la littérature mais sont conformes aux écrits existants et sont le résultat d'un travail de validation avec les chargés de formation pratique.

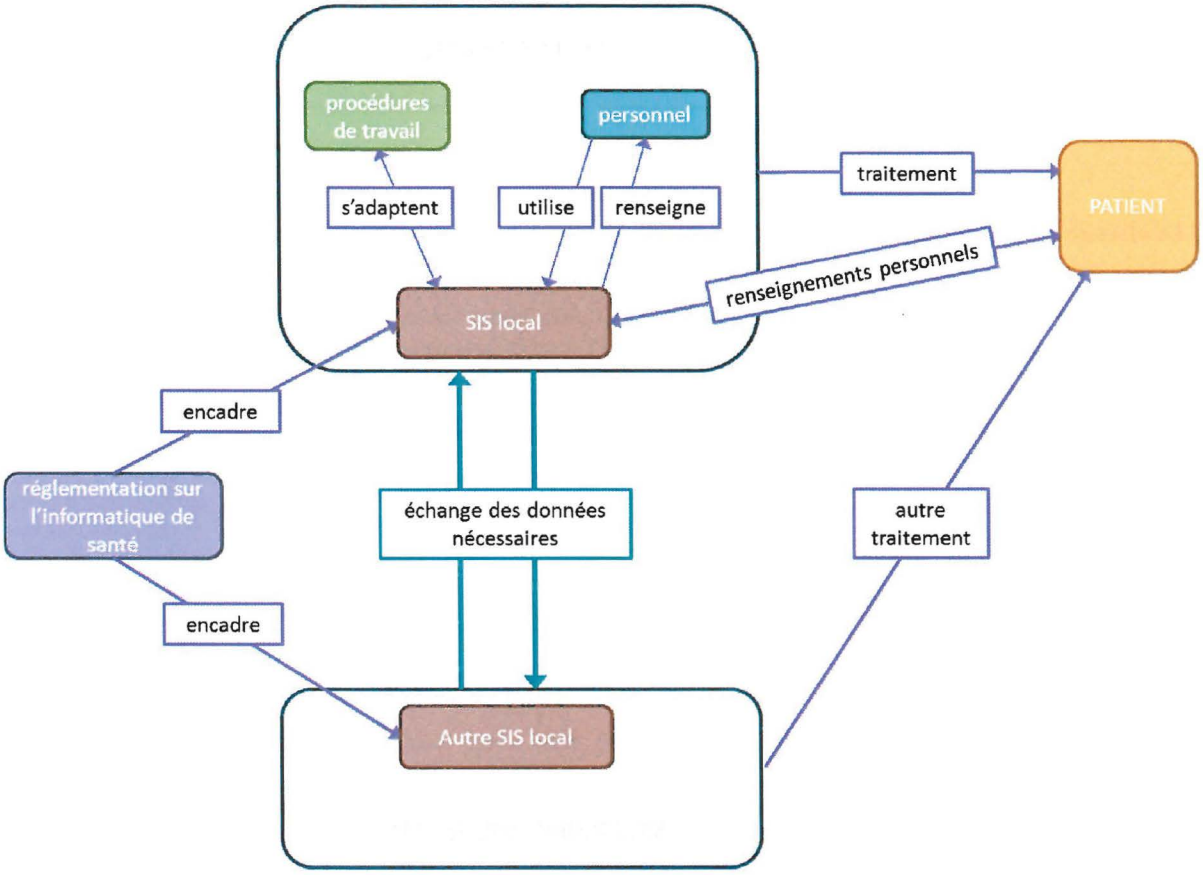
1. Les Systèmes Informatiques de Santé (SIS)

La gestion des informations n'est pas née d'un seul coup avec l'avènement des systèmes informatiques. Bien avant et depuis toujours, les organisations de santé doivent gérer les données sur leurs patients, sur les traitements, les médicaments... Aujourd'hui, en lieu et place de moyens plus classiques tels que les formulaires papiers, sont de plus en plus utilisés les outils informatiques, électroniques et de télécommunication, tant et si bien qu'on parle d'informatisation de la santé.

L'implantation d'un système informatique de santé (SIS) s'inscrit donc dans un plus large système préexistant, dont le but est de traiter les patients. La justification à l'ajout de l'outil informatique dans ce processus est d'améliorer sa performance en termes financiers ou en ce qui concerne la sécurité des patients puisque plusieurs dysfonctionnements ou non rentabilité ont pu apparaître avec le temps(Morgan, 2004) (Bates, et al., 1999).

L'implantation d'un SIS dans une organisation influe sur les pratiques, il doit pouvoir s'adapter aux façons de faire pour ne pas nuire au traitement des patients, mais il entraine forcément des modifications de certaines procédures et l'ajout de certaines tâches dans les processus de travail en place (Ash, Berg, & Coeira , 2004). Les interactions entre le SIS et le personnel sont multiples : celui-ci ajoute des informations dans le SIS au fur et à mesure que les traitements sont effectués, mais le SIS donne aussi des informations qui sont utiles pour le traitement.

Schéma de la situation : avec quoi interagit le SIS ?



Vis-à-vis des patients, on stocke de l'information personnelle sur eux, ce qui engage leur vie privée. De ce fait, de nombreuses réglementations viennent encadrer les SIS sur la protection de ces données, sur la sécurité intrinsèque de l'outil ou encore sur d'autres aspects. Quand les patients se font traiter à un autre endroit, les données peuvent être récupérées par la nouvelle organisation (par exemple, le service d'urgence d'un hôpital qui a besoin des informations recueillies par le médecin de famille). En disposant des informations du patient, le traitement pourra être plus adéquat, et on pourra par exemple, éviter de faire des tests en double et connaître les médicaments pris par le patients, ses allergies, ses antécédents et bien plus.

Cet échange peut se faire grâce à des connexions entre les SIS locaux, ou bien par un SIS d'un niveau supérieur, une grande base de données alimentée par les SIS locaux, auquel les intervenants peuvent accéder depuis n'importe quelle organisation. On peut donc avoir des SIS communs à une région, une province ou même un pays. (Institute of Medicine, 2012)

Différentes formes de SIS

Bien qu'une recension exacte de toutes les applications des SIS n'est pas disponible, il est possible de présenter les outils les plus courants qui peuvent être inclus dans les systèmes utilisés aujourd'hui tels que (Institute of Medicine, 2012):

- ***Entrée Informatisée des Ordonnances Médicales (EIOM)*** : Outil qui sert à gérer les ordonnances et prescriptions via l'informatique.

- ***Aide à la décision*** : Outils qui permettent aux praticiens d'aller chercher des informations médicales qui peuvent aider à prendre une décision pour le traitement. Par exemple, on peut disposer d'un registre des médicaments et des doses standards. Cela peut aussi prendre la forme d'alertes en cas de risques d'interactions entre plusieurs traitements ou de risques d'allergies

- ***Dossier électronique*** : Outil qui permet de stocker des informations sur un patient en particulier. La forme électronique a comme valeur ajoutée que le dossier peut être partagé plus facilement lorsqu'un patient est traité à des endroits différents et par plus d'un professionnel de la santé.

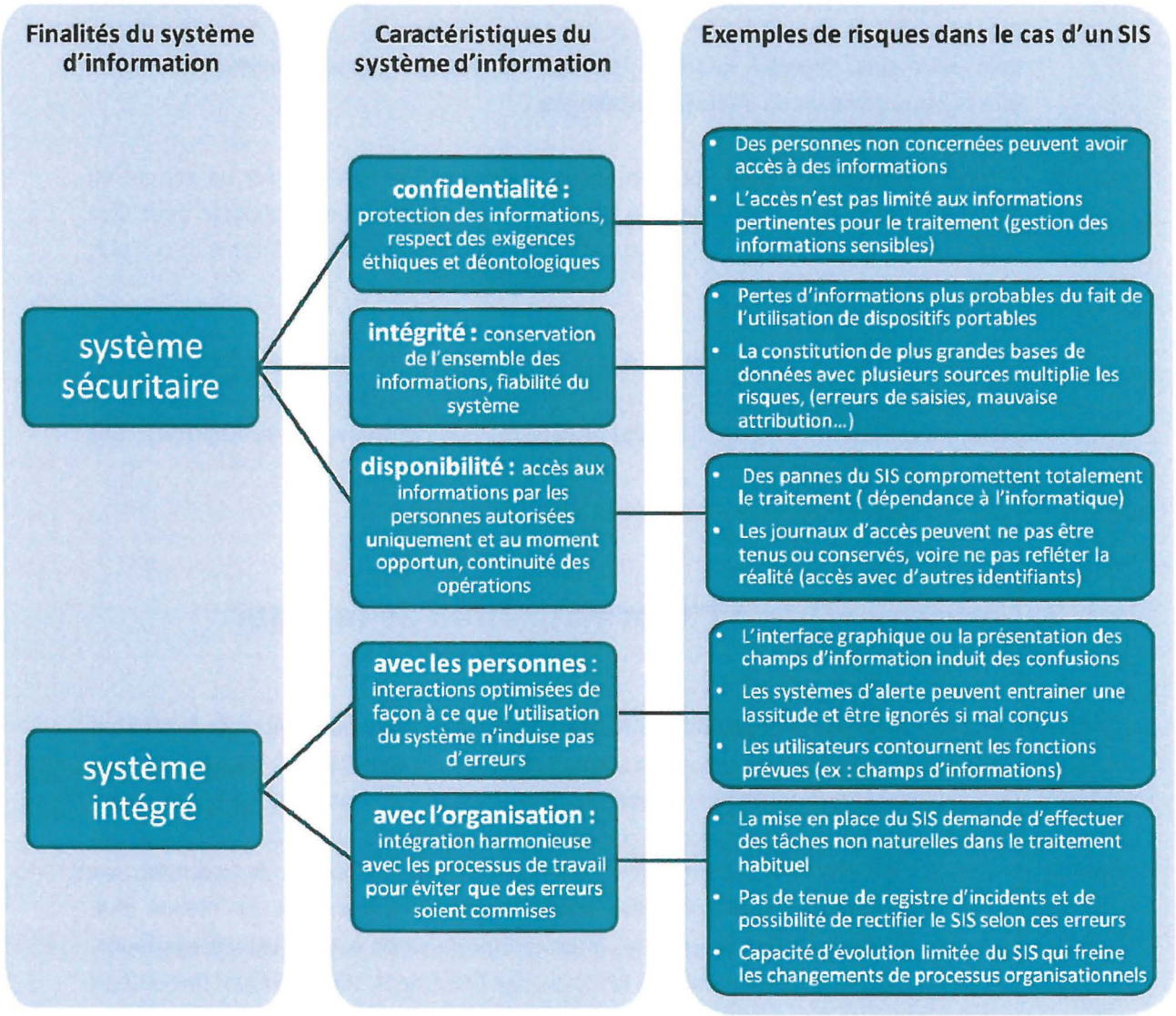
- ***Outils d'implication des patients*** : Ce sont souvent des plateformes qui permettent aux patient de consulter les informations recueillies sur eux, voire même de participer plus activement à leur traitement, dans des projets que l'on regroupe dans la littérature sous le terme de télémédecine.

2. Les risques liés à l'informatisation de la santé

Plusieurs avantages de l'introduction des nouvelles technologies dans les services de santé sont mis en avant par des groupes de médecins supporteurs des technologies ou par les pouvoirs publics qui encouragent leur utilisation (comme le gain de temps, la rentabilité ou la baisse des accidents sur la sécurité ou la vie privée des patients), mais puisque la plupart des introductions de SIS ne sont pas encore bien documentées , il est difficile de mesurer et de quantifier ses avantages, et encore moins leurs possibles inconvénients. Il s'agit tout de même d'un changement majeur dans la façon de gérer les informations de santé et avec ces changements, la structure de risques liés à l'information de santé change forcément. Alors que certains risques diminuent voire disparaissent, on est aussi confrontés à de nouveaux risques ou à d'autres qui

sont accrus. Ces risques peuvent entraîner des dangers sur l'ensemble des éléments se rapportant au système d'information, autant pour l'organisation, son personnel ou les patients traités.

Dans ce schéma, sont décrites les deux finalités principales que tout système d'informatisation (informatique ou non) se doit d'avoir, c'est-à-dire qu'il permet de gérer les informations de façon sécuritaire et qu'il est intégré adéquatement dans l'environnement dans lequel il fonctionne. A partir de ces finalités, on peut déterminer quels sont les caractéristiques d'un système d'information performant. Les risques peuvent venir s'appliquer à l'une ou l'autre ce ces caractéristiques. Ici, sont présentés des risques qui sont imputables à un système d'information utilisant l'outil informatique :



Si on se place dans le cas d'un SIS, c'est-à-dire d'un système d'information de santé qui utilise les outils informatiques, les finalités restent les mêmes qu'auparavant. Mais pour chacune d'entre elles, des risques apparaissent au moment où on passe à un système informatique, qui eux sont spécifiques à l'utilisation d'un SIS. Les différentes caractéristiques de des systèmes d'information apparaissent être une bonne façon de regrouper les différents risques, en l'absence d'une typologie fonctionnelle présente dans les écrits sur le sujet. Ces caractéristiques sont souvent amenées dans la définition d'un SIS (American National Standards Institute, 2012), (Office of the National Coordinator for Health Information Technology, 2012) mais ne sont habituellement pas utilisées à des fins de typologies de risques.

Une revue de littérature a permis de documenter des exemples de risques reliés aux SIS, et de les classer selon la typologie retenue (avec les caractéristiques d'un système d'information) afin de valider ce choix :

- ***Exemple d'un cas de bris de confidentialité dû au SIS*** (Sinnema, 2011) **:** Une pharmacienne chez Zellers à Edmonton, a utilisé le réseau de dossiers provinciaux Netcare pour consulter l'historique médical de 8 personnes de son entourage avec qui elle avait un différend personnel. Ces personnes se sont rendu compte du bris de confidentialité au moment où la coupable a partagé des informations sensibles et personnelles sur le réseau social Facebook.

- ***Exemple d'un incident touchant l'intégrité des informations dans un SIS*** (Dell, 2012)**:** On parle ici d'une compagnie d'assurance des États-Unis qui a dû payer en 2009 des millions de dollars (1 million pour vérifier qu'il n'y ait pas de vol d'identité, plus de 500 000 $ en courriers et amendes et plus encore de dommages pour l'image de l'entreprise). La compagnie a en effet perdu (ou s'est fait volé…) un disque dur externe contenant des informations sur 1.5 millions de clients. Ce qui a été critique dans ce cas est que la compagnie avait négligé de protéger les informations sur ce genre de dispositifs mobiles par des systèmes de cryptage, les données étaient donc directement accessibles.

- ***Exemple de dangers liés à la disponibilité de l'information dans un SIS*** (Campbell, Sittig, Ash, Guaponne, & Dykstra, 2006) **:** Les auteurs rapportent plusieurs erreurs induites par l'apparition de la technologie dans le monde de la santé dont une touchant à la disponibilité de l'information dans un SIS. Ils expliquent que nombreux sont les jeunes médecins qui n'ont été formés qu'avec les outils d'aide à la décision. S'ils savent

très bien s'en servir ce qui est un point très positif, on remarque par contre que lorsqu'ils arrivent dans une petite organisation qui ne dispose pas de tels systèmes ou lorsque qu'il y a une panne quelconque du SIS (qui peut durer plusieurs heures), ils ne savent plus faire certaines tâches, ne se souviennent plus des doses standards des médicaments ou des contre-indications, des remplacements possibles en cas d'allergies etc... La technologie devient une partie indispensable des soins alors qu'elle ne l'était pas auparavant, on appelle ce phénomène la dépendance à la technologie.

- ***Exemple d'une erreur induite par l'interface SIS/humain*** (Horsky, Kuperman, & Patel, 2005) : Cet article revient sur un incident survenu au New-York Presbyterian Hospital. Il s'agit d'un patient qui arrive avec un taux bas de potassium, qui est traité en lui administrant des doses de potassium par intraveineuse. Du fait d'incohérences dans le système d'EIOM, deux prescriptions sont en fait données et le calcul de la dose totale est faussé ce qui entraine l'administration de trop de potassium. Pire encore, le lendemain un deuxième médecin consulte les résultats du patient, mais ce sont les résultats de la veille qui s'affichent et pensant que le patient a toujours un taux trop bas de potassium le médecin fait une nouvelle prescription, ce qui a rendu le patient hyperkaliémique.

- ***Exemple d'erreurs induites par un manque d'ajustement du SIS avec les procédures en place*** (Ash, Berg, & Coeira , 2004) : Les auteurs rapportent un problème courant appelé «the midnight problem». Il s'agit de patients arrivant dans la nuit, qui voient un médecin avant minuit, qui fait une prescription pour le lendemain, et le temps que le dossier soit traité par le SIS, il est après minuit et la prescription pour le lendemain est en fait programmée pour le surlendemain ce qui laisse le patient un jour complet sans prescription et sans médication.

Méthodologie de la recherche

Questions de recherche

Les questions de recherche déjà abordées au moment de l'introduction, sont maintenant reprises et énoncées avec plus de précision :

- Quel est l'avancement des pays retenus dans la mise en place de SIS et quel est le contexte entourant leur démarche d'informatisation de la santé ?
- Quels sont les risques perçus par les pays et quelles mesures ont-été prises dans ces pays pour y faire face ?
- Comme s'y prendre ou comment s'y est-on déjà pris pour évaluer des mesures liés aux risques posés par les SIS, quel est précisément le problème et les variables touchées ?

Méthode de cueillette des données

Dans ce travail, la méthodologie de recherche a été avant tout l'analyse de la documentation officielle disponible. Les documents sont essentiellement rassemblés via les sites Internet officiels des organisations responsables de l'implantation des SIS dans les gouvernements respectifs comme des ministères ou des agences publiques, ou encore d'organisations internationales comme l'Union Européenne ayant fait le portrait de ses membres sur le sujet de l'informatisation de la santé. Certains documents sont aussi des études (publiées dans des revues scientifiques) ou encore des prises de positions (d'associations de patients, de médecins ou d'instituts spécialisés) recueillis dans les ressources des centres documentaires du MSSS et de l'ENAP. Les documents ont été choisis, selon leur pertinence vis-à-vis du sujet. La plupart des documents consultés se trouvent listés dans la bibliographie de ce document.

Cette méthode a été choisie du fait qu'il n'était pas possible (ni réellement utile) de se déplacer dans les différents pays pour les comparer en faisant des analyses de terrain ou des entrevues en personne. De plus, de nombreuses informations sont disponibles via les sites Internet officiels des organisations publiques, ce qui a permis d'étudier 6 pays dans le temps imparti pour le stage.

Mais l'analyse documentaire effectuée ici a pourtant quelques défauts : d'une part, l'accès aux documents est limité à ce à quoi les organisations veulent bien mettre en ligne. Certains documents peuvent ne pas être disponibles au public, ou non présentés sur le site internet de

l'organisation ou du ministère concerné. D'autre part, une seconde limite est celle de la langue, notamment pour le Danemark ou l'Estonie, ou les documents consultés ne sont que ceux qui ont été traduits.

Mais dans l'ensemble du travail, on peut tout de même considérer que ces limites ne constituent pas une trop forte entrave à la validité des résultats, l'ensemble des informations nécessaires, surtout à l'analyse comparative ont été trouvées. Par contre, et ceci est vrai pour l'ensemble des pays, même au Canada, les données dont on dispose proviennent avant tout des organisations en charge de la gestion des programmes d'informatisation de la santé. On ne dispose que de très peu d'information sur la réception et l'utilisation des technologies par les médecins ou les patients autant dans la littérature scientifique que par d'autres mediums. Pour recueillir ce type de renseignements, on ne peut pas faire uniquement appel à la documentation et il faudrait pouvoir faire des entrevues avec les acteurs concernés ce qui ne rentrait pas dans le mandat de stage. Cela dit cette méthode différente aurait pu enrichir les observations sur les pays, et peut-être permettre de se rendre jusqu'à faire des recommandations sur les meilleures pratiques à adopter.

Résultats de la recherche

Comme cela est présenté dans la description du mandat, la recherche se divise en deux parties. Tout d'abord, il y a eu l'étude des pays et notamment leur avancement en ce qui concerne l'informatisation de la santé et leur réactions face aux risques. L'analyse comparative complète est présentée en annexe. Ici ne figure qu'un résumé par pays, ainsi que des tableaux synthèses. A la fin de l'analyse, certaines conclusions tirées de la comparaison des pays sont énoncées. En seconde partie, sont présentées des perspectives d'évaluation en matière d'informatisation de la santé, de façon générale, puis un exemple est ensuite cité pour appliquer la méthodologie à un cas concret. Pour finir, comme pour la première partie, plusieurs conclusions sont tirées des perspectives d'évaluation.

1. Analyse comparative des pays choisis

En annexe, figure l'analyse comparative complète. Celle-ci regroupe quelques chiffres de présentation des pays, qui permettent aussi de mieux les comparer. Pour chaque pays ensuite, se trouvent une partie sur l'avancement en termes d'informatisation de la santé pour contextualiser les données sur les risques. La dernière partie , la plus importante porte sur les risques perçus par les pays et les mesures prises pour y faire face. L'angle utilisé pour recenser ces mesures est la typologie des risques présentée précédemment, qui regroupe ces derniers selon les caractéristiques d'un système d'information performant. L'ensemble de ces mesures est enfin présenté sous forme de tableaux synthèses afin de rendre la comparaison plus aisée.

Résumés par pays

Canada, niveau fédéral et niveau provincial

Au Canada, malgré le fait que ce soit les provinces qui soient responsables de l'organisation des services de santé, le gouvernement mets en place des incitatifs pour les encourager fortement à investir dans l'informatisation de la santé, notamment dans le but de mettre en place un dossier santé à l'échelle Canadienne. Les provinces ont des niveaux d'avancement dans l'implantation

des SIS plutôt différents : l'Alberta dispose déjà d'un dossier provincial, d'autres comme la Colombie-Britannique, l'Ontario et le Québec sont aussi à l'étape de mise en œuvre.

Le gouvernement fédéral, par l'entremise de son organisme Inforoute Santé Canada, donne une certification pour s'assurer de la sécurité des SIS et demande aux provinces d'en faire une évaluation de la confidentialité. Pour le reste, les provinces ont leurs propres règles de sécurité alliant listes de critères pour recevoir du financement, certifications, ententes de confidentialité... L'implantation encore récente des SIS permet d'expliquer en partie que les préoccupations de confidentialité, d'intégrité, de disponibilité ou sur l'interface organisation/système ou humain /systèmes ne soient pas encore étudiées en profondeur.

Danemark

Le Danemark est un pays qui a beaucoup d'expérience dans l'implantation des SIS, et ce notamment auprès des médecins de famille, première ligne du traitement au patient. Plus récemment, ont été développés des systèmes d'ampleur nationale, comme des EIOM et des dossiers à l'échelle du pays. Il est intéressant de noter que l'organisation qui a géré l'introduction des SIS, Medcom, est d'origine privée, même si aujourd'hui, elle est financée par des fonds publics. Ce contexte explique pourquoi il y a peu de réglementations de sécurité, vues comme des entraves au développement de l'innovation issue de la sphère privée. Mais Medcom propose aussi une certification, et la confidentialité des données est assurée grâce à des contrôles exercés par les patients eux-mêmes, sur un portail Internet, regorgeant de fonctionnalités.

Estonie

L'Estonie n'est pas un pays qu'on penserait d'instinct comme porteur de modernité et d'informatisation et pourtant il s'agit d'un des pays utilisant le plus les nouvelles technologies dans la prestation des services publics. Au niveau de la santé, comme pour d'autres services, le système mis en place est de conception publique, et regroupe autant des dossiers locaux, nationaux, de prescription électronique et d'aide à la décision. Pour la sécurité des SIS, on se focalise beaucoup sur les menaces venant de l'extérieur, les stratégies de sécurité étant communes aux services publics. La confidentialité des données, sensée être protégée par plusieurs mesures reste encore floue pour plusieurs médecins.

France

La France a un passé d'informatisation de la santé, mais uniquement à des fins de facturation et remboursement. Un peu comme au Canada, on investit depuis quelques années pour

l'implantation des SIS dans le but de moderniser la santé et de trouver plus d'efficience. Depuis peu, un système de dossier national a été mis en place, pour l'instant sur la base du volontariat. Comme au Danemark, le patient a accès à un portail lui permettant de gérer son dossier, notamment pour le contrôle des accès. La France possède des réglementations de sécurité plutôt originales, très récemment sur l'interface humain/système des EIOM, ou sur les hébergeurs de données. Certaines parties de la sécurité ne sont par contre pas encore vraiment circonscrites, mais une politique générale est en cours d'écriture.

Nouvelle-Zélande

A l'instar du Danemark, la Nouvelle-Zélande a informatisé son système de santé depuis longtemps, et notamment sous l'influence du domaine privé. De même, ce sont les médecins dans leurs cabinets qui ont été les premiers dotés de SIS, aujourd'hui ont suivis un système de prescription électronique a suivi ainsi qu'un dossier national, en cours d'implantation. Les réglementations de sécurité n'ont pas été très présentes à l'introduction des SIS, du fait qu'il s'agissait au départ d'initiatives plutôt régionales. Aujourd'hui plus de règles se développent autour de la sécurité des SIS, sous la forme de normes et de standards introduits par un organisme plutôt original du fait qu'il agit par normalisation : HISO.

États-Unis

Aux États-Unis, l'informatisation est clairement associée à l'administration Obama, qui souhaite moderniser le monde de la santé. On passe par l'incitation des organisations de santé à adopter les SIS, en offrant des remboursements, dès lors que le système est implanté selon des critères de bonne utilisation appelés Meaningful Use. Au sein de ces critères, qui évoluent au cours du temps, s'inscrivent des mesures de sécurité, qui touchent à la fois le système en lui-même, mais aussi l'environnement dans lequel il est implanté, comme le respect de la confidentialité pour les employés et dans les procédures. Les États-Unis ont aussi un grand souci des risques associés aux SIS, des bris de confidentialité qui sont rendus publics, aux nouveaux risques, notamment sur l'interface humain/système, dont l'IOM propose une étude approfondie en vue de nouvelles réglementations, (Institute of Medicine, 2012).

Tableaux synthèse

Afin de mieux se représenter les résultats de la recherche, les tableaux suivants regroupent toutes les initiatives prises par les États analysés pour contrer les risques liés à l'informatisation de la santé. Ceux-ci sont répartis selon la typologie retenue pour les risques, à savoir les caractéristiques d'un système d'information performant.

Famille de risques	Canada (niveau fédéral)	Alberta	Ontario	Colombie-Britannique
Risques liés à la disponibilité de l'information	• Certifications des SIS sur le marché	• Vendor Conformance and Usability Requirements, liste de critères à laquelle les répondants aux appels d'offres de SIS doivent se conformer • Publication des non conformités	• Certification selon les critères Spec 4.1 • Politique sur la sécurité de l'information (reprenant les normes ISO 27001 et 27002) • Guides pour petites et grandes organisations	• 4 vendeurs certifiés grâce des critères posés en appel d'offre. Obligation de sélectionner un vendeur certifié pour bénéficier d'un remboursement • « Liste des choses à faire » pour les médecins et organisations de santé pour être éligible au programme de remboursement • Dossier national confié entièrement à une firme privée et obligation de publication des incidents de sécurité ou confidentialité • Nouvelle loi sur la protection des données personnelles en santé électronique
Risques liés à l'intégrité des données				
Risques liés à la confidentialité des données	• Évaluation des facteurs relatifs à la vie privée des SIS demandée aux provinces	• Privacy Impact Assesment, engagement au respect de la part des professionnels et des organisations, et sanctions en cas de non respect	• Politique sur les incidents touchant la vie privée et la confidentialité. • Protection intégrée de la vie privée • Bureau de protection de la vie privée	
Risques liés aux interactions avec les personnes	• Guides de bonnes pratiques, services de soutien	• Formations pour le personnels disponibles	• Programme et services d'aide à la mise en place d'un SIS	• Service d'aide à l'implantation et échange de bonnes pratiques via des forums ou communautés de pratiques
Risques liés aux interactions avec les processus de travail		• Équipe de soutien aux organisations pour l'intégration des SIS		

Famille de risques	Danemark	Estonie	France	Nouvelle-Zélande	Etats-Unis
Risques liés à la disponibilité de l'information	• Certification de l'ensemble des SIS sur la marché	• Système entièrement développé par les autorités publiques • Loi sur l'organisation des services de santé qui reconnaissent que l'intégrité, la disponibilité et la confidentialité doivent êtres respectées • Protection des données publiques contre les cyberattaques	• Politique de sécurité en cours de rédaction • Agrément des hébergeurs de données de santé obligatoire • Décret sur la confidentialité des données du dossier national • Possibilité pour les patient de gérer les accès à leurs dossiers	• Guide de normes de sécurité de l'information formulés par le HISO • Réflexions sur la certification des SIS	• Analyse de sécurité obligatoire dans les critères « Meaningful Use » • Certification des SIS déléguée à des firmes privées
Risques liés à l'intégrité des données					
Risques liés à la confidentialité des données	• Loi sur l'utilisation des données personnelles • Tenue des registres d'accès et échantillons vérifiés aléatoirement • Accès des patients à un portail permettant de gérer les accès aux données			• Loi sur les renseignements personnels de santé	• Loi sur la protection des données de santé • Publication des bris de confidentialité concernant plus de 500 patients
Risques liés aux interactions avec les personnes	• Certification contenant des critères sur la présentation des items		• Certification des EIOM par la Haute Autorité de Santé	• Réflexion sur la certification des SIS	• Réglementation sur la formation du personnel • Institute of Medecine mandaté d'une étude sur ce type de risques, recommandations formulées mais non encore appliquées
Risques liés aux interactions avec les processus de travail					

Bilan de l'analyse comparative

L'étude de ces différents pays, avancés en termes d'informatisation de la santé nous permet de tirer plusieurs conclusions sur le niveau de réglementation des risques et l'évolution de la prise en compte de ces risques :

- ***Confidentialité : suffisamment réglementée ?*** Tout d'abord, on remarque qu'au moment d'introduire un SIS, les risques concernant la confidentialité sont souvent les premiers à être abordé et réglementés. C'est en effet, une préoccupation fondamentale dans le domaine de la santé qui a toujours été importante pour les patients, qui voient depuis longtemps la garantie de la confidentialité dans leur traitement incluse dans la déontologie médicale. Ainsi, on remarque que l'ensemble des pays disposent de législations sur la confidentialité des données médicales. Pourtant si on reconnaît que les risques de bris de confidentialité sont différents avec l'utilisation des nouvelles technologies et évoluent, souvent, la réglementation est conçue et adoptée au moment de l'implantation et n'est pas ou peu rectifiée par la suite. Or, il est difficile d'identifier tous les problèmes de confidentialité potentiels dès le départ et dans de nombreux cas, des améliorations ne sont souvent possibles qu'avec le recul (en allant notamment recueillir l'avis des praticiens qui utilisent la technologie à tous les jours). Autre exemple, les mesures prises pour protéger la confidentialité des données sont souvent prises en fonction d'un élément extérieur (comme une cyber-attaque), alors que de nombreux bris de confidentialité proviennent l'interne (Protti D. , 2004). Cette autre sorte de menace à la confidentialité, souvent sous-évaluée, demande des mesures de protection des données différentes, mais aussi de nouvelles façons de se rendre compte et de contrôler les abus. D'autres menaces proviennent de l'évolution continue des technologies et de leur environnement. Par exemple les SIS deviennent plus mobiles (clés USB, tablettes, téléphones intelligents...) ce qui pose constamment de nouveaux enjeux de protection de la confidentialité non pris en compte par des lois plus anciennes, alors que de plus en plus de personnes s'inquiètent du respect de leur vie privée avec l'implantation des nouvelles technologies. (Collier, 2012)

- ***Intérêt porté uniquement sur les patients*** : Un autre point intéressant est le fait que toutes les inquiétudes soulevées sur la confidentialité et sur les changements de la pratique médicale apportés par l'implantation des SIS sont concentrées sur les risques pour le patient. On ne parle que peu de la mutation de la pratique pour les médecins : des dossiers qui n'étaient d'abord visibles que par leur auteur, peuvent aujourd'hui être consultés par un certain nombre dans leurs confrères, ce qui engendre forcément un certain nombre de

changements de comportement pour les médecins. Il y a aujourd'hui surement une place pour ce genre de témoignage et pour la documentation de ces questions, mais elles ne prennent pas encore leur place dans le débat sur les SIS.

- ***Grandes différences en sécurité de l'information*** : Les risques qui concernent la disponibilité ou l'intégrité sont gérés de façons assez différentes. Certains États ont de fortes législations pour contraindre les vendeurs de SIS à considérer ces aspects de sécurité dans leur conception. D'autres pays par contre laissent plus de latitude au marché, les médecins et hôpitaux sont les clients et c'est à eux de faire leur demande en termes de sécurité aux vendeurs. On peut dire que cette deuxième façon de faire est plus courante dans les pays ayant une plus longue habitude des SIS, où ils sont implantés depuis plus longtemps (Danemark, Nouvelle-Zélande) et où la législation trop forte a plutôt été perçue comme un frein à l'informatisation.

- ***Émergence des questions sur l'intégration harmonieuse des SIS*** : L'intégration du SIS dans les organisations de santé combinées aux comportements et aux habitudes des humains ainsi que les risques qu'elles occasionnent deviennent des questions de plus en plus en émergence : c'est à la fois un sujet nouveau et qui intéresse beaucoup les chercheurs en informatique de santé. On se rend compte que des erreurs que l'on qualifiait souvent d'erreurs humaines sont induites en grande partie par la technologie. Les recherches récentes se concentrent de plus en plus sur l'ergonomie des interfaces des SIS ou sur la personnalisation et l'adaptation des SIS de base à chaque organisation pour mieux répondre à ses besoins et s'ajuster aux processus en place. (Borycki, Kushniruk, Keay, Nicoll, Anderson , & Anderson , 2009) (Phansalkar, et al., 2010). On dénombre encore peu de législations majeures dans ce sens même si des initiatives commencent à naître et qu'on assiste à des prises de conscience grâce aux recherches de plus en plus nombreuses.

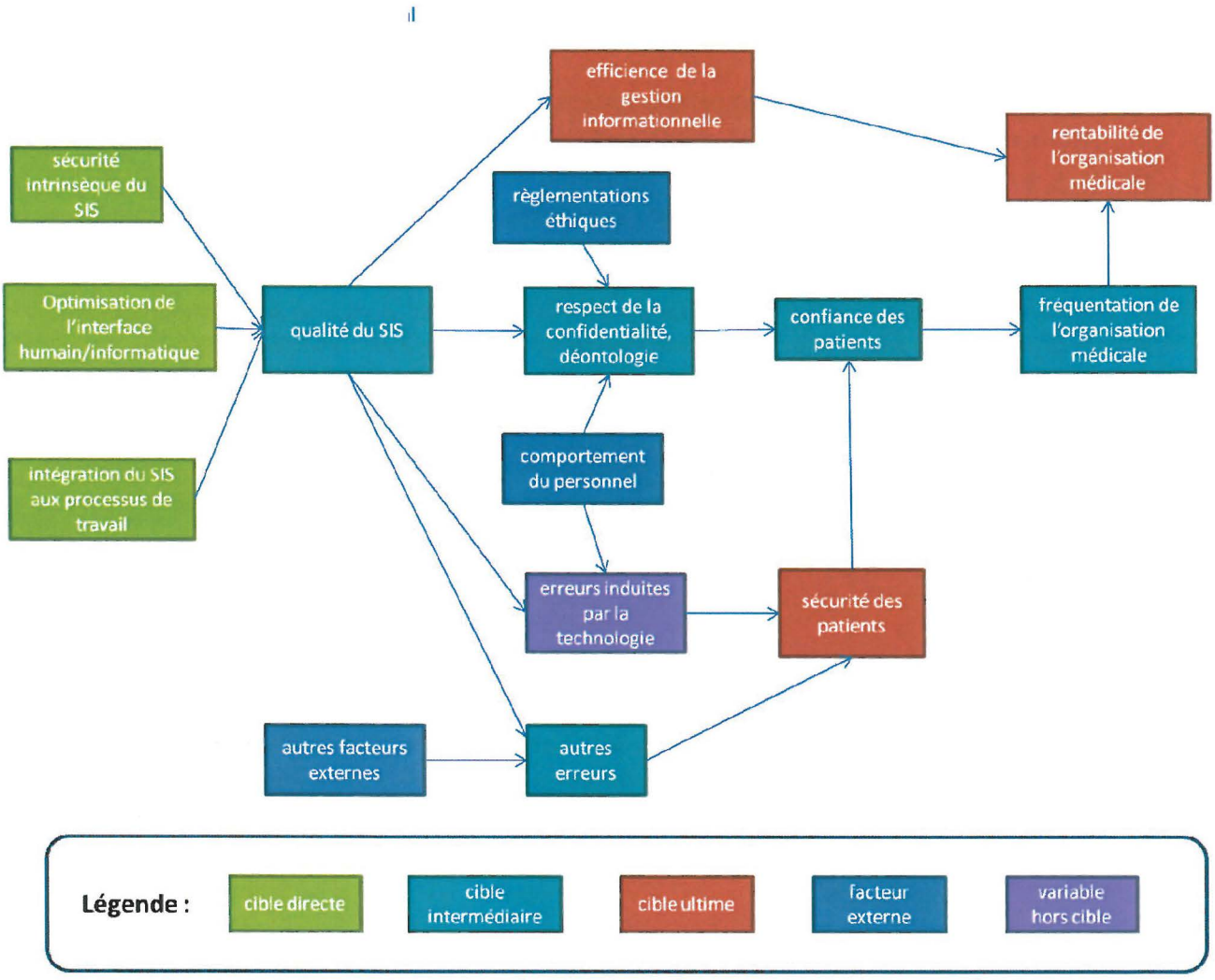
2. Perspectives d'évaluation des mesures prises

Afin de justifier les dépenses en informatisation de santé, nombreuses sont les organisations publiques qui affirment que cette solution rend la gestion informationnelle plus efficace et que cela augmente la sécurité des patients en réduisant le nombre d'erreurs médicales commises (cyberSanté Ontario, 2012a) (IT health board, 2012).

Pourtant, lorsque l'on va chercher dans la littérature sur le sujet, plusieurs chercheurs indiquent que peu de preuves formelles ont été avancées jusqu'à présent pour prouver les avantages apportés par l'informatisation de la santé (Protti D. , 2004), (Institute of Medicine, 2012). En effet, l'introduction des nouvelles technologies entrainant aussi certains risques, erreurs, des changements dans les pratiques habituelles, des pertes de temps et de gros investissements, il n'est pas si évident d'affirmer qu'il s'agit de la solution pour rendre les organisations de santé plus efficaces. Dans ce contexte, il est intéressant de se pencher sur les possibilités d'évaluation dans ce domaine, afin de mieux se rendre compte de l'impact de l'arrivée des technologies de l'information dans la santé.

Schéma de problématique général

Pour commencer à aborder la problématique de l'informatisation de la santé du point de vue de l'évaluation de programmes, un schéma de problématique peut être utile. Ce schéma représente la problématique générale de l'informatisation de la santé. Une mesure peut ne toucher qu'une seule partie de la chaîne causale. Un exemple concret suivra pour mieux comprendre comment il est possible d'agir sur ce problème.



Dans ce schéma c'est le niveau de qualité du SIS qui est central. Il est déterminé par plusieurs caractéristiques, précédemment exprimées comme étant des finalités du SIS. Pour des fins de simplification du modèle les trois caractéristiques renvoyant à la sécurité (disponibilité, intégrité et confidentialité) ont été regroupées sous l'item « sécurité intrinsèque ».

La qualité d'un SIS a une incidence sur les erreurs médicales commises lors du traitement. Selon les justifications apportées par les autorités publiques, l'implantation d'un SIS de qualité va permettre de réduire le nombre d'erreurs médicales appelées ici «autres erreurs» (cyberSanté Ontario, 2012a), mais va aussi entrainer de nouvelles erreurs, appelées «erreurs induites par la technologie» (Borycki, Kushniruk, Keay, Nicoll, Anderson , & Anderson , 2009). Ensembles, ces deux types d'erreurs auront des conséquences sur la sécurité des patients dans l'épisode de traitement, ce qui va positivement ou négativement affecter la confiance des patients en l'organisation médicale. (American National Standards Institute, 2012)

La qualité du SIS influence aussi le respect des normes de déontologie et de confidentialité dans le traitement, même si elle n'en est pas le seul déterminant. D'après plusieurs recherches récentes, le respect de la déontologie est un facteur important dans la confiance des patients, à tel point que cela conditionne en partie la fréquentation d'une organisation médicale (Fairwarning, 2011).

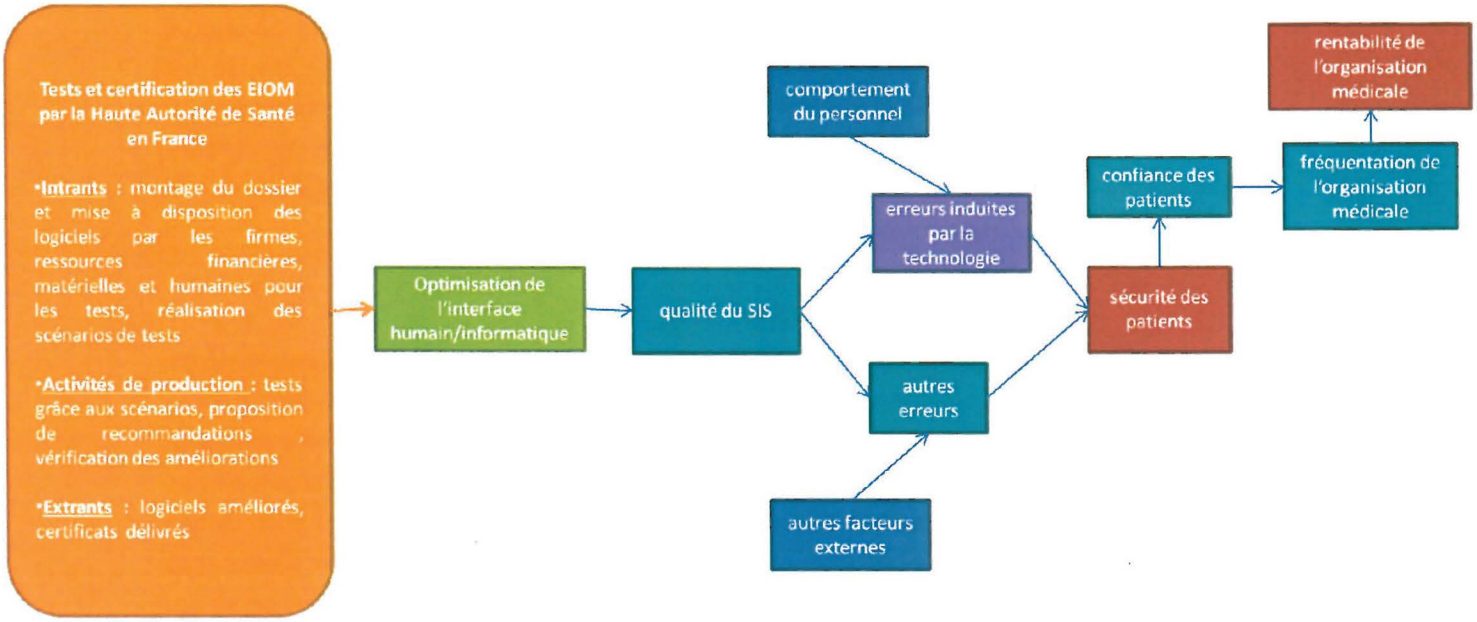
En dernier lieu, un SIS de qualité permet de modifier l'efficience de la gestion informationnelle dans une organisation médicale. En effet, et c'est un point souvent cité comme justification à l'implantation des SIS, l'informatique permet souvent aux médecins de sauver du temps (Alberta Health and Wellness, 2012b), ce qui leur permet de dégager du temps supplémentaire de consultation (certains témoignages indiquent que les médecins peuvent voir 10 à 20 % de patients en plus en une journée). Cet élément, de même que la fréquentation de l'établissement influent tous deux la rentabilité de l'organisation médicale.

Modèle causal : exemple d'application à une mesure existante

- **Mesure choisie** : Tests et certification des EIOM par la Haute Autorité de Santé en France

L'exemple retenu concerne la chaîne causale de la sécurité des patients. Il s'agit d'une mesure visant à réduire le nombre d'erreurs induites par la technologie et qui passe par la cible de l'interface homme/SIS. Comme il a été dit plus tôt, les EIOM sont souvent des sources d'erreurs de prescriptions, notamment du fait d'une conception qui n'est pas optimisée. (Bates, et al., 1999) Pour réduire ces erreurs qui représentent potentiellement un grand danger pour les patients, la HAS Française a décidé de tester les systèmes d'EIOM disponibles sur le marché, notamment leur ergonomie et leur façon de détecter les interactions médicamenteuses.

1



Ce modèle causal dé montre bien que cette certification ne permet de toucher qu'une partie de la chaine causale rattachée à la qualité des SIS, celle de la sécurité des patients. Afin de mesurer les effets d'une telle mesure, la variable centrale à considérer est celle des erreurs induites par la technologie. Pour mesurer cette variable, il est essentiel de pouvoir séparer les erreurs qui sont commises pendant les soins et d'isoler celles qui sont induites par la technologie et donc de créer un réel suivi des erreurs médicales avec l'analyse de leurs causes. Il est aussi possible de réaliser des tests d'erreurs sur les EIOM pour savoir s'ils sont susceptibles d'induire des erreurs ou non, comme l'ont déjà fait plusieurs chercheurs (Borycki & Keay, 2010). Avec ce genre de tests, on peut vraiment voir l'effet "avant-après" de la mesure en réalisant un test avant le processus de certification et un après, une fois que les modifications recommandées ont été effectuées. Par contre, la limite de ces tests est qu'ils ne reflètent pas toujours la réalité de l'utilisation sur le terrain, pouvoir travailler sur les vrais rapports d'erreurs serait préférable.

Bilan des perspectives d'évaluation

- Certaines variables de notre schéma de problématique rendent l'évaluation assez aisée puisqu'elles sont disponibles ou facilement mesurables, comme la fréquentation des organisations médicales ou encore l'efficience de la gestion informationnelle. En effet, il est possible de mesurer le temps passé par les professionnels de santé sur la gestion des informations et se rendre compte des effets de l'introduction d'une technologie, ou d'une autre mesure. Du fait de cette facilité de mesure, ces effets souvent positifs sont très fréquemment mis en avant (par exemples, les gains de temps pour les médecins de famille qui peuvent recevoir plus de patients par jour...).

- L'évaluation des effets de mesures de sécurité touchant les SIS implique de pouvoir mesurer d'autres variables clés dans le schéma de problématique. C'est notamment le cas des erreurs induites par la technologie ou des autres erreurs qui peuvent être évitées grâce à la technologie ou encore des cas de bris de confidentialité. Or de nos jours, on remarque que l'on dispose de très peu de données quant aux sources des erreurs médicales (on ne pourrait par exemple que difficilement déterminer si elles sont induites par la technologie ou non), mais plutôt des récits factuels sur ce qui se passe. Dès lors, il est difficile autant de mesurer ces phénomènes à des fins d'évaluation, et encore plus de pouvoir établir un cycle de corrections de la pratique suite aux erreurs commises.

- Un certain mouvement s'élève parmi les praticiens et les chercheurs pour introduire un environnement plus enclin à l'amélioration et à l'apprentissage des erreurs qui ont été commises. On appelle ce type d'environnement, une culture juste (« just culture ») (Institute of Medicine, 2012). Comme les auteurs du rapport de l'IoM le soulignent, cette façon de penser est applicable à la sécurité des SIS. Il s'agit de faire un rapport systématique des erreurs, et de ce qui les a causées, pour pouvoir créer un cercle vertueux d'améliorations. Pour ce faire, il faut que chacun se sente à l'aise de rapporter les erreurs qui se sont produites durant son travail sans être menacé de sanctions. Les gestionnaires doivent encourager le rapport des erreurs et non punir les auteurs, sans quoi les rapports seront moins nombreux. Avec les données de chaque erreur documentées, il sera possible d'en savoir plus sur la part des erreurs induites par les technologies, sur les bris de confidentialité sur les autres types d'erreurs, et de proposer des changements afin que ces incidents ne se reproduisent pas.

Conclusion

Grâce à cette étude, on peut se rendre compte que le mouvement d'informatisation de la santé ne s'est pas fait de façon uniforme dans tous les pays. De grandes disparités sont notés dans la façon dont se sont implantés les SIS, et dans la façon dont la sécurité est prise en compte. La littérature sur le sujet permet de se rendre compte de cette diversité des SIS disponibles mais les informations sur les risques sont plus éparses. En effet, les risques entourant ces systèmes émergeants sont causés par tout un environnement et non juste par le SIS en tant que tel. Il pourrait dès lors s'avérer bien difficile de formuler des recommandations qui soient valables pour plusieurs établissements ou encore dans l'ensemble des pays, tellement ils ont leurs caractéristiques propres.

On peut toutefois être certain que les États n'en sont pas au même stade de prise de conscience sur les problèmes de sécurité posés par les SIS. Alors que dans certains pays les ajustements réglementaires pris lors des premières implantations de systèmes informatiques sont considérés comme suffisants et ne sont pas retouchés par la suite, d'autres s'engagent dans des discussions sur les nouvelles catégories de risques qui apparaissent et qui ont rendus de plus en plus publics, notamment par la communauté des chercheurs. Un partage de ces nouvelles interrogations pourrait être tout à fait bénéfique pour les autres pays, dans lesquels les mêmes problèmes se posent obligatoirement (confidentialité, interface entre l'homme et le système...).

Dans cette prise de conscience des risques posés par les SIS l'évaluation de programme peut jouer un rôle important. En effet, cette dernière suppose que les évaluateurs disposent de données sur la gestion et les résultats des SIS. Et ceci passe donc par une meilleure connaissance des changements apportés par l'informatisation de la santé, incluant ces risques nouveaux. Et ce n'est qu'avec cette meilleure connaissance, qu'un mouvement de prévention du risque et d'amélioration pourra s'enclencher.

Bibliographie

Alberta Health and Wellness. (2012a). *Netcare Portal.* Consulté en juin 2012, sur http://www.albertanetcare.ca/

Alberta Health and Wellness. (2012b). *POSP Website.* Consulté en juin 2012, sur http://www.posp.ab.ca/

American National Standards Institute. (2012). *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security.*

Ash, J., Berg, M., & Coeira , E. (2004). Some Unintended Consequences of Information Technology in Health Care : The Nature of Patient Care Information System-related Errors. *Journal of the American Medical Information Association , 11*, pp. 104-112.

ASIP Santé . (2012b). *Site Web du DMP.* Consulté en juin 2012, sur http://www.dmp.gouv.fr/web/dmp/

ASIP Santé. (2012a). *Site Web de l'ASIP Santé.* Consulté en juin 2012, sur http://esante.gouv.fr/

Bates, D., Teich, J., Lee, J., Seger, D., Kuperman, G., Ma'Luf, N., et al. (1999). The impact of Computerized Physician Order Entry on medication error prevention. *Journal of the American Medical Informatics Association , 6* (4), pp. 313-321.

BC eHealth Strategy Council. (2011). *Health Sector Information Management/Information Technology Strategy 2010/11 - 2012/13.* Ministry of Health of British Columbia.

Borycki, E., Kushniruk, A., Keay, E., Nicoll, J., Anderson , J., & Anderson , M. (2009). Toward an integrated simulation approach for predicting and preventing technology-induced errors in healthcare: implications for decision-makers. *Healthcare Quaterly , 12*, pp. 90-96.

Campbell, E., Sittig, D., Ash, J., Guaponne, K., & Dykstra, R. (2006). Types of Unintended Consequences Related to Computerized Provider Order Entry. *Journal of the American Medical Informatics Association , 13* (5), pp. 547-556.

Collier, R. (2012). Medical privacy breaches rising. *Canadian Medical Association Journal , 184* (4), pp. E215-E216.

cybersanté Ontario. (2011). *Politique sur la confidentialité des renseignements.*

cybersanté Ontario. (2012b). *Politique sur la sécurité de l'information.*

cyberSanté Ontario. (2012). *Site Web de l'agence cyberSanté Ontario*. Consulté en juillet 2012, sur http://www.ehealthontario.on.ca/fr/

cyberSanté Ontario. (2012a). *Site Web de l'agence cyberSanté Ontario*. Consulté en juillet 2012, sur http://www.ehealthontario.on.ca/fr/

Danish Ministry of Health. (2012). *eHealth in Denmark.*

Dell. (2012). *Doing More with Mobile Devices in Healthcare: Eliminating the Security Compromise*. Récupéré sur Site Web de l'entreprise Dell Canada: http://content.dell.com/ca/en/corp/d/corp-comm/mobile-devices-in-healthcare

Estonian ICT Export Cluster. (2012). *Site e-Estonia*. Consulté en juin 2012, sur http://e-estonia.com/

European Commision. (2010). *eHealth Strategies, Country brief : Estonia.*

European Commission. (2010). *eHealth Strategies, Country Brief : Denmark.*

European Commission. (2010). *eHealth Strategies, Country brief : France.*

Fairwarning. (2011). *Canada: How privacy considerations drive patient decisions and impact patient care outcomes ?*

HAS. (2012). *Site Web de la Haute Autorité de Santé*. Consulté en juin 2012, sur http://www.has-sante.fr/portail/jcms/j_5/accueil

Health Policy Monitor. (2010). *'Meaningful Use' of Electronic Health Records.*

Health Policy Monitor. (2010). *National Health Information system - follow up, Estonia.*

HISO. (2012). *HISO 10029.1 Health Information Security Framework, Essentials and Recommendations.*

Horsky, J., Kuperman, G., & Patel, V. (2005). Comprehensive analysis of a medication dosing erros related to CPOE. *Journal of the American Medical Informatics Association , 12* (4), pp. 377-382.

Inforoute Santé Canada. (2011). *Rapport Annuel 2010-2011 «Vers l'étape utlime... De l'accessibilité à l'adoption».*

Inforoute Santé Canada. (2012). *Site Web d'inforoute santé Canada*. Consulté en juin 2012, sur https://www.infoway-inforoute.ca/index.php/fr/

Institute of Medicine. (2012). *Health IT and Patient Safety : building safer systems for safer care.* Washington, DC: The National Academies Press.

IT health board. (2012). Consulté le juillet 2012, sur National Health IT Board's Website: http://www.ithealthboard.health.nz/

Medcom. (2012). *Site Web de l'organisation Medcom en anglais*. Consulté en mai 2012, sur http://www.medcom.dk/wm109991

Ministry of Health of BC. (2007). *PLIS and iEHR Project Summary.*

Ministry of Health, BC. (2012). *Site Web du ministère de la santé de la Colombie Britannique, section santé électronique*. Consulté en juillet 2012, sur http://www.health.gov.bc.ca/ehealth/

Morgan, M. (2004). In pursuit of a safe Canadian healthcare system. *Healthcare Papers , 5* (3), pp. 10-26.

National Health IT Board. (2010). *National Health IT Plan.* New Zealand.

OCDE. (2011). Consulté en juillet 2012, sur le Site Web de l'OCDE, section statistiques: http://www.oecd.org/document/0,3746,fr_2649_201185_46462787_1_1_1_1,00.html

Office of the National Coordinator for Health Information Technology. (2012). *Guide to Privacy and Security of Health Information.*

Ontario MD. (2012). *Site Web de l'organisation Ontario MD*. Consulté en juillet 2012, sur https://www.ontariomd.ca/portal/server.pt/community/home/205

Patient First. (2011). *FAQ on NZ ePrescription Service.* Récupéré sur http://www.patientsfirst.org.nz/wp-content/uploads/2011/11/NZePS-Questions-Answers-2011-10-17.pdf

Phansalkar, s., Edworthy, J., Hellier, E., Seger, D., Schedlbauer, A., Avery, A., et al. (2010). A review of human factors principles for the design and implementation of medication safety alerts in clinical information systems. *Journal of the American Medical Informatics Association , 17*, pp. 493-501.

Physician Information Technology Office. (2012). *Site Web du Programme PITO de la Colombie Britannique*. Consulté en juillet 2012, sur http://www.pito.bc.ca/

Protti, D. (2004). Patient Safety : Is the Evidence Strong Enough That Information Technology Can Help ? *Healthcare Papers , 5* (3), pp. 37-42.

Protti, d., Bowden, T., & Johansen, I. (2008). Adoption of information technology in primary care physician office in New Zealand and Denmark. *Informatics in Primary Care* (16,17).

Sinnema, J. (2011, Décembre 6). Edmonton pharmacist fined $15K for posting medical records to Facebook during spat with church group. *National Post* .

Annexe

Annexe 1 : analyse comparative complète, extraite du rapport produit pour le MSSS

ANALYSE COMPARATIVE

Le Canada

Tableau 3 : Informations sur la santé au Canada (OCDE, 2011)

Canada	
Population	**33 909 700**
Espérance de vie	**80,7 ans**
Nombre de médecins (par 1 000 hab.)	**2,4**
Nombre de lits d'hôpital (par 1 000 hab.)	**3,3**
Dépenses de santé (par habitant, $US PPP)	**4363**
Dépenses de santé (en % du PIB)	**11,4%**
Part du financement public	**70,6%**

Niveau fédéral

La santé électronique au Canada

Au Canada, ce sont les provinces qui sont responsables de l'organisation de la santé, le niveau fédéral n'a donc a priori pas l'initiative en matière d'informatisation de la santé. Mais, pour encourager l'adoption des SIS, qui ne sont pas aussi fréquents que dans les pays les plus avancés, le gouvernement fédéral propose du financement aux provinces.

C'est l'organisme indépendant «Inforoute Santé Canada» qui gère les initiatives de santé électronique depuis 2001. Il agit en tant qu'investisseur des fonds du gouvernement fédéral pour des projets de SIS, souvent conjointement à des investissements provinciaux. Le but ultime est que chacune des provinces se dote d'un dossier médical provincial, dans des normes définies au départ qui permettront de les interconnecter pour avoir un dossier à l'échelle du pays.

En plus du financement proposé, Inforoute Santé Canada offre plusieurs services pour la mise en place des solutions de santé électronique, œuvre dans le partage des expériences et des bonnes pratiques et surveille aussi que l'implantation se fait dans de bonnes conditions.

Il est intéressant de noter que les subventions fédérales ne sont versées qu'après que certaines fonctionnalités soient mises en place, ainsi la part de subventions versée est un bon indicateur de l'avancement des projets dans les différentes provinces.

Les réactions face aux risques au Canada

La première mesure de sécurité dont s'occupe Inforoute Santé Canada est la certification des SIS offerts sur le marché. Cette certification se base sur des critères élaborés à partir de normes nationales et internationales comme l'ISO 27001 ou l'ISO 17799. Ces critères se structurent selon des grands thèmes que sont la confidentialité, la sécurité mais aussi l'interopérabilité et la gestion. Les opérations de certification n'incluent explicitement aucune appréciation de la «convivialité» des solutions.

Pour compléter les vérifications à propos de la confidentialité, Inforoute demande à ce que les projets qu'elle finance fassent l'objet d'une évaluation des facteurs relatifs à la vie privée (EFVP). Cette évaluation n'est pas faite par Inforoute directement mais par les administrations qui demandent du financement, il n'y a donc pas de façon fixe de la faire, cela dépend des différentes administrations.

Il n'y a pas beaucoup d'autres réglementations encadrant les risques des SIS au niveau fédéral, mais certains services de soutien sont quand même offerts par Inforoute Santé Canada. On peut notamment citer un service de conseil en gestion du changement, pour accompagner le passage à l'informatisation, qui regroupe une trousse d'outils pratiques, un cadre de travail et un forum qui peut permettre l'échange de bonnes pratiques.

Sources : (Inforoute Santé Canada, 2012), (Inforoute Santé Canada, 2011)

Niveau provincial : Alberta

La santé électronique en Alberta

La province de l'Alberta figure parmi les précurseurs au Canada puisqu'elle a implanté un dossier médical à l'échelle provinciale qui s'appelle Netcare. Il regroupe plusieurs informations sur les patients (informations démographiques, traitements prescrits, allergies et immunisations, test de laboratoire ou rapports d'imagerie...) mais pas toutes celles qui sont contenues dans des dossiers locaux détenus par les hôpitaux ou les médecins de famille. Par contre les données sélectionnées sont automatiquement transférées des dossiers locaux au dossier provincial.

Il comporte aussi plusieurs outils d'aide à la prise de décision comme des alertes sur les interactions entre différents traitements ou une base de données sur tous les médicaments existants et les dosages standards.

Par contre, ce n'est pas cet outil du niveau provincial qui permet de gérer les ordonnances, et il n'y a pas encore d'outil où les patients peuvent consulter librement leur dossier, ils doivent en faire la demande là où ils sont traités et il y a souvent des frais pour y accéder.

En plus du SIS provincial qu'est Netcare, existent les SIS locaux, chez les praticiens, les hôpitaux... Les fournisseurs sont multiples, ce qui explique qu'on a différents SIS locaux qui cohabitent. On peut toutefois noter que pour recevoir des aides du gouvernement pour l'implantation d'un SIS (Programme POSP), il faut choisir un des trois fournisseurs autorisés (Telus Physician Solutions, Med Access ou MD Physician Services). Ces trois fournisseurs proposent des produits variés et on ne peut généraliser sur les SIS implantés dans la province, mais à la fois l'EIOM, l'aide à la décision et les dossiers électroniques font partie des fonctions disponibles.

Les réactions face aux risques en Alberta

Les actions réglementaires encadrant les divers SIS se concentrent essentiellement autour des risques liés à la sécurité des informations. Le règlement principal gérant l'informatique de santé est la «Health Information Act» (HIA).

En ce qui concerne la disponibilité et l'intégrité des données, des règles précises sont imposées aux concepteurs des SIS. Les trois entreprises sélectionnées pour le programme POSP ont dû satisfaire à une liste d'exigences appelée VCUR : «Vendor Conformance and Usability Requirements», mis à jour en 2008. De plus, des critères de disponibilités et d'intégrité tout au

long de l'utilisation sont définis et à chaque fois qu'un SIS sort de ces critères et que le concepteur ne peut pas régler la situation dans des délais prescrit, il y a une publication du problème assortie de sanctions pouvant aller jusqu'à la rupture du contrat.
Les entités stockant des données et qui veulent se connecter au portail Netcare doivent passer par une sorte de certification : «Provincial Organizational Readiness Assessment» (PORA) qui garantit que les critères de la HIA sont respectées.

Au niveau de la confidentialité, il y a différents niveaux d'accès qui correspondent aux besoins des différents professionnels («need-to-know basis») dans le portail Netcare. Par exemple un employé administratif n'aura pas accès aux données médicales mais seulement aux données démographiques). De plus, chaque organisation et professionnel qui souhaite recevoir du financement pour l'implantation ou se connecter au réseau Netcare doit remplir une sorte d'engagement de respect de la vie privée («Privacy Impact Assessment») prévue dans la HIA, en expliquant la gestion qui sera faite pour garantir la confidentialité des données, et suivre une formation au sujet du respect de la vie privée. Il y a des sanctions prévues en cas de comportement contraire à cette déclaration. Par contre la tenue d'un registre des bris de confidentialité n'est pas obligatoire, seulement encouragée dans le cadre de bonnes pratiques.

On peut toutefois remarquer que quelques actions s'attachent aux risques liés à la qualité du SIS et notamment sur les interactions avec les procédures de travail, puisqu'il existe une équipe («Alberta Netcare EHR Portal Deployment Team») qui s'occupe d'aider la mise en place du SIS provincial Netcare par des formations du personnel, ou en offrant de l'assistance pour créer la liaison entre le SIS local et Netcare.

Sources: (Alberta Health and Wellness, 2012a), (Alberta Health and Wellness, 2012b)

Niveau provincial : Ontario

La santé électronique en Ontario

En Ontario, une agence indépendante du Ministère de la Santé et des Soins de longue durée a été créée pour gérer les projets de santé électronique : cyberSanté Ontario. Les missions de cette agence sont de relier les SIS existants, notamment par un dossier, comme le préconise Inforoute Santé Canada. Avant cela, d'autres initiatives d'interconnexion ont été lancées telles qu'un système d'échange de données neurologiques, d'imagerie médicale ou encore des systèmes de gestion des malades atteints de maladies chroniques. Ces échanges se font grâce à

un système d'interconnexion géré par cyberSanté Ontario qui s'appelle One Network, accessible par des SIS locaux ou via Internet.

Pour ce qui concerne le dossier provincial plus particulièrement, même si son architecture, son contenu ou encore la réglementation autour de lui se construit, il n'est pas encore en vigueur. Il s'agit plus de la prochaine étape dans la stratégie de santé électronique de l'Ontario. Par contre les projets de prescription électronique sont avancés, des projets pilotes ont été réalisés, les médecins peuvent consulter un visualiseur de profil pharmaceutique qui leur permet d'avoir des renseignements sur les médicaments et leur possibles dangers ou contre-indications, et sur l'historique pharmaceutique de leur patients. Avec les leçons de ces projets, se dessinera le futur système de gestion des médicaments à l'échelle provinciale.

D'autre part, il existe une autre structure dans les projets d'informatisation de la santé, qui elle gère les programmes d'aide financière pour les médecins afin qu'ils se dotent de SIS locaux: Ontario MD, créée avec l'appui de l'association des médecins. Grâce à ces initiatives, les dossiers locaux sont bien implantés puisque 8 millions d'Ontariennes et d'Ontariens en disposent.

Les réactions face aux risques en Ontario

Les responsabilités en matière de sécurité des SIS sont partagées entre les deux organisations citées précédemment.

Pour les SIS locaux, c'est Ontario MD qui gère la sécurité de l'information. Il a été choisi d'imposer une certification des SIS, réalisée par l'organisation pour s'assurer de la qualité des SIS proposés. Cette certification se présente sous la forme d'une liste de critères à remplir, appelés «specifications». Cette liste est mise à jour périodiquement pour améliorer la qualité demandée, en avril de cette année on est d'ailleurs passé de Spec. 3.0 à Spec 4.1. De plus, il existe un programme pour aider les médecins à faire leur transition vers l'informatique de santé, qui les aide notamment à trouver le SIS qui leur convient, à le mettre en place et à bien l'utiliser.

Pour tout le reste c'est plutôt cybersanté Ontario qui s'occupe de sécurité de l'information. L'organisation dispose d'ailleurs de plusieurs politiques, une sur la sécurité de l'information (qui se base directement sur les normes ISO 27001 et 27002), une sur la gestion des incidents touchants la protection de la vie privée et une sur la confidentialité. cybersanté Ontario a aussi mis en place un bureau de protection de la vie privée qui s'occupe d'appliquer les réglementations en vigueur comme la Loi de 2004 sur la protection des renseignements personnels sur la santé. Il est intéressant d'étudier la gestion des risques effectuée par ce bureau : ils ont en effet développé une méthode de «protection intégrée de la vie privée», c'est-

à-dire que toutes les étapes, toutes les parties du SIS, tous les services, produits et procédures doivent être pris en compte et non seulement l'utilisation du SIS dans son sens restreint. Enfin, cybersanté Ontario propose aussi des services d'aide à la transition vers l'informatique de santé, ainsi que des guides de sécurité de l'information autant pour les petites que les grandes organisations de santé.

Sources : (cyberSanté Ontario, 2012a), (Ontario MD, 2012), (cybersanté Ontario, 2011) (cybersanté Ontario, 2012b)

Niveau provincial : Colombie-Britannique

La santé électronique en Colombie-Britannique

En Colombie-Britannique, le Ministère de la Santé dispose d'un Conseil sur la Stratégie en Santé électronique qui gère les activités liées à l'informatisation de la santé. C'est ce conseil qui a rédigé les documents d'orientation comme la stratégie qui couvre la période 2010 à 2013 (Health Sector Information Management/Information Technology Strategy).

En suivant cette stratégie générale, plusieurs initiatives ont été lancées pour atteindre les objectifs. La première étape est de soutenir l'adoption des dossiers médicaux locaux chez les médecins qui est un préalable à tout autre projet d'envergure. Cette aide se fait depuis 2007 par le PITO (Physician Information Technology Office) qui gère les investissements prévu dans le «Physician Master Agreement» qui est un accord qui a été passé avec l'association des médecins pour aller vers l'informatisation de la gestion de l'information dans les cabinets des médecins.

Un autre projet en cours est celui de constituer un dossier médical provincial, dans le but de le connecter aux dossiers des autres provinces, c'est pourquoi il est nommé iEHR (interoperable Electronic Health Record). Sa conception est laissée sous contrat à la firme Sun Microsystems. Au sein de ce grand projet s'insère d'autres initiatives, telles que le PLIS (Provincial Laboratory Information Solution) qui va servir de répertoire pour tous les résultats de laboratoire dans la province. Le dossier iEHR va aussi inclure un système de prescription électronique : PharmaNet-

eRx, qui va améliorer le système PharmaNet existant, permettant déjà de prévenir les mauvaises interactions entre plusieurs médicaments, et de gérer le remboursement des médicaments.

Pour terminer le tour d'horizon des initiatives en informatisation de la santé on peut mettre en avant les projets de télésanté dans plusieurs domaines (TeleThoracic, TeleOncology,

TeleOphtalmology...) ou l'application Panorama, qui est un système d'information sur l'état de santé de la population.

Les réactions face aux risques en Colombie-Britannique

La sécurité en ce qui concerne les SIS locaux utilisés par les médecins est gérée par le PITO. Ce dernier a tout d'abord mis en place une certification des systèmes. En fait, un peu comme cela s'est fait en Alberta, grâce à un appel d'offres, certains vendeurs jugés conformes aux critères de départ sont sélectionnés. Pour être éligibles aux programmes de remboursements des investissements en santé électroniques, les médecins doivent choisir un SIS chez un des quatre vendeurs certifiés.

Pour que les médecins puissent recevoir leurs remboursements, certaines mesures doivent avoir été prises, y compris en ce qui concerne le respect de la vie privée et la sécurité des informations. C'est sous forme d'une liste de choses à faire que les médecins sont invités à remplir l'ensemble des critères menant à l'éligibilité au programme d'aide. Parmi ces éléments, citons la gestion des identifiants des utilisateurs du SIS, la mise en place d'une procédure fixe pour gérer les incidents, ou la nomination d'un responsable de la sécurité. Pour toutes ces tâches, le PITO propose un service d'aide à l'implantation, et encourage les médecins à échanger leurs bonnes pratiques via des forums, des parrainages ou des communautés de pratiques.

En ce qui concerne le dossier médical provincial iEHR, tout le volet sécurité et confidentialité est confié au contractant Sun Microsystems. Ce dernier est tenu de reporter tout incident autant dans la sécurité que dans des bris de confidentialité. D'autres clauses obligent Sun Microsystems à héberger les données uniquement au Canada ou encore de former son personnel à la sécurité de l'information.

Enfin la Colombie-Britannique a mis en place un nouveau cadre législatif pour la gestion des données par les SIS : la eHealth Personal Health Information Access and Protection of Privacy Act, qui s'ajoute à d'autres lois déjà existantes sur la protection des renseignements personnels. Cette nouvelle loi décrit les accès possibles au dossier provincial, limités au minimum selon les besoins des différents professionnels (chaque profession a un rôle différent auquel correspondent certains accès). On y souligne aussi la possibilité pour les patients d'accéder à leur dossier et de bloquer l'accès à certaines données s'ils le veulent.

Sources: (BC eHealth Strategy Council, 2011), (Ministry of Health of BC, 2007), (Physician Information Technology Office, 2012), (Ministry of Health, BC, 2012)

Le Danemark

Tableau 4 : Informations sur la santé au Danemark (OCDE, 2011)

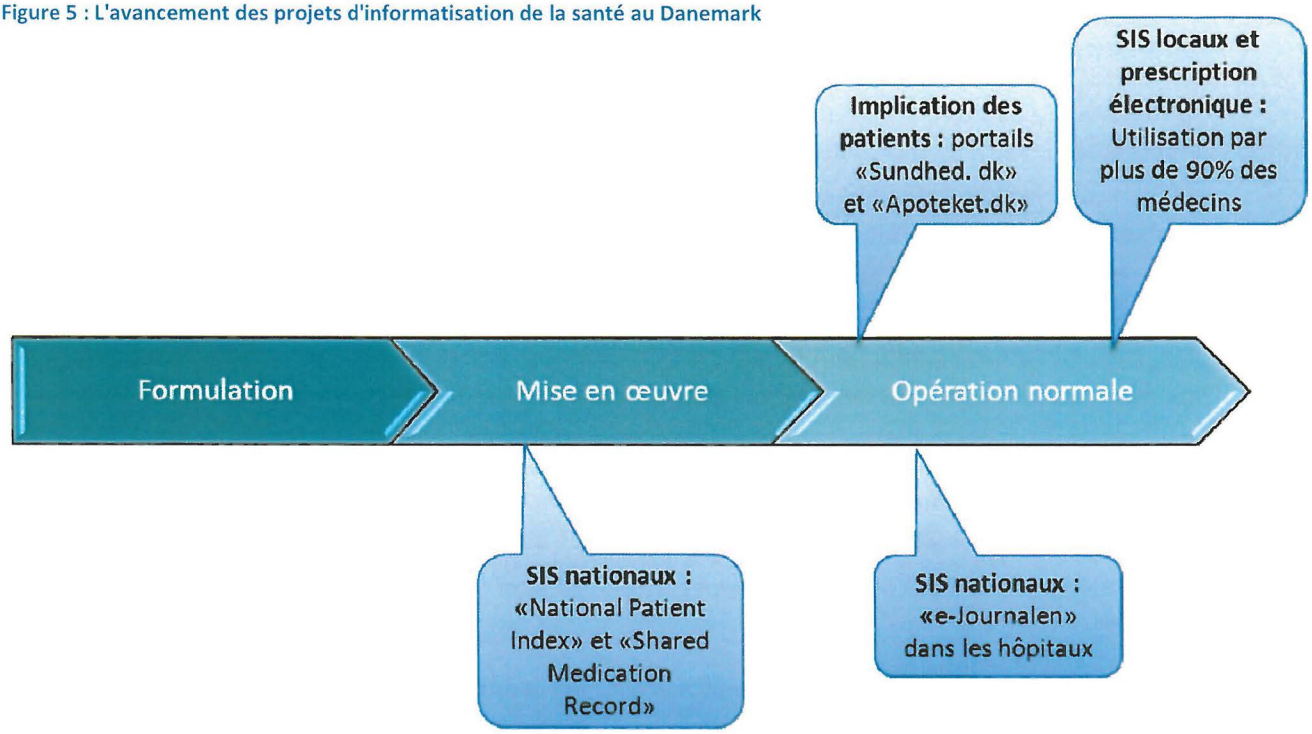
Danemark	
Population	**5 495 246**
Espérance de vie	**79 ans**
Nombre de médecins (par 1 000 hab.)	**3,4**
Nombre de lits d'hôpital (par 1 000 hab.)	**3,5**
Dépenses de santé (par habitant, $US PPP)	**4348**
Dépenses de santé (en % du PIB)	**11,5%**
Part du financement public	**85,0%**

La santé électronique au Danemark

Comme on peut le remarquer sur la Figure 1, le Danemark est déjà bien avancé dans l'informatisation de son système de santé. Les médecins de famille, qui forment la première ligne des soins, sont équipés depuis de nombreuses années en SIS locaux. Les outils d'EIOM sont bien implantés, en association avec les pharmaciens depuis au moins 2007 ce qui fait que les prescriptions sont en grande partie gérées via l'informatique. Les hôpitaux possèdent aussi leurs propres SIS depuis autant d'années.

Les projets les plus récents au Danemark touchent plus les liaisons entre ces différents SIS existants, dans le but de créer des dossiers électroniques nationaux, qui fourniront un éventail complet d'information sur les patients, autant sur les médicaments qu'ils prennent, leurs hospitalisations antérieures, leurs résultats de test ou d'imagerie, leurs vaccins ou allergies, mais aussi leurs souhaits en ce qui concerne la réanimation ou le don d'organes.

Figure 5 : L'avancement des projets d'informatisation de la santé au Danemark



La partie qui touche la liaison des SIS dans les hôpitaux a été achevée, le tout étant disponible pour les patients sur le portail Sundhed.dk, qui regroupe aussi une mine d'informations, de forums sur la santé et qui permet de communiquer, de prendre rendez-vous avec son médecin et même de consulter les listes d'attente pour divers soins. Les autres projets qui permettront d'achever de constituer des dossiers longitudinaux des patients, de leur naissance à leur décès en sont encore à leur phase d'implantation, qui doit se terminer en 2013.

Les réactions face aux risques au Danemark

La première instance gérant l'informatisation de la santé est l'Agence Nationale de Santé Électronique, qui se place directement sous la responsabilité du Ministère de la Santé du Danemark. Elle produit les lois et règlements encadrant la santé électronique et initie des programmes d'envergure nationale. Elle s'occupe aussi de répandre des bonnes pratiques de gestion.

Une des tâches principales de l'Agence Nationale de Santé Électronique ces derniers temps a été de développer des standards pour les SIS afin de réduire le nombre total de SIS pour s'assurer d'une gestion, d'une plus grande disponibilité des données et pour faciliter l'interconnexion (on

veut passer de 27 SIS en 2011 à 5 pour les hôpitaux en 2013 et réduire le nombre de SIS locaux proposés par 11 vendeurs différents).

Une autre organisation importante est Medcom, qui a rassemblé au moment de sa création des organismes publics et privés. Aujourd'hui, elle est financée uniquement par les administrations publiques de niveau national, régional et local. C'est un organisme central pour la mise en place des solutions d'informatisation de santé, qui gère notamment depuis 2000 la certification des différents SIS. La certification qui dure une semaine, s'intéresse à la fonctionnalité, à l'interopérabilité, à la conformité aux standards ou encore à la présentation des items dans les SIS. Elle est donnée ensuite pour une durée illimitée, tant que le SIS n'est pas modifié de façon majeure. Les standards utilisés sont surtout ceux issus des modèles européens CEN.

En ce qui concerne la réglementation autour des SIS, on considère que le Danemark n'a pas eu de lois trop dures afin de ne pas faire obstacle au progrès technologique. Plusieurs lois encadrent tout de même la pratique comme la Loi de Santé de 2007 ainsi que la Loi sur l'Utilisation de Données Personnelles qui est gérée par l'Agence Danoise pour la Protection des Données.

Le point le plus réglementé concerne la protection des données personnelles. La règle générale est qu'on peut recueillir de l'information sans consentement sur un patient mais il doit en être informé et il a le droit de se retirer du système. On a par contre besoin d'une preuve de consentement du patient pour aller chercher des données sur un patient dans une base de données que ce soit pour un usage médical ou non (administration, recherche...) La seule exception à cette règle est que le consentement explicite n'est pas requis pour l'accès par un professionnel au cours d'un épisode de soins. C'est-à-dire qu'au moment du traitement, si on est en charge d'un patient, on peut aller chercher de l'information pertinente dans son dossier électronique, mais pas en dehors de cette fenêtre de temps. Pour contrôler ces accès des registres doivent être tenus et des échantillons de ces journaux sont vérifiés aléatoirement pour s'assurer qu'il n'y a pas de mauvaise utilisation des SIS.

De leur côté, les patients peuvent accéder à leurs données et demander l'interprétation de celles-ci par un médecin de façon gratuite. Ils peuvent aussi masquer certaines données ainsi que refuser l'accès à certains professionnels. Pour protéger leur accès et contrôler leur identité en entrant sur le portail Internet, le patient dispose d'un identifiant avec le système «NemID» qui permet un accès sécurisé aux services électroniques de santé mais aussi à d'autres services publics et des services bancaires par internet.

Sources: (Danish Ministry of Health, 2012), (European Commission, 2010), (Protti, Bowden, & Johansen, 2008), (Medcom, 2012)

L'Estonie

Tableau 5 : Informations sur la santé en Estonie (OCDE, 2011)

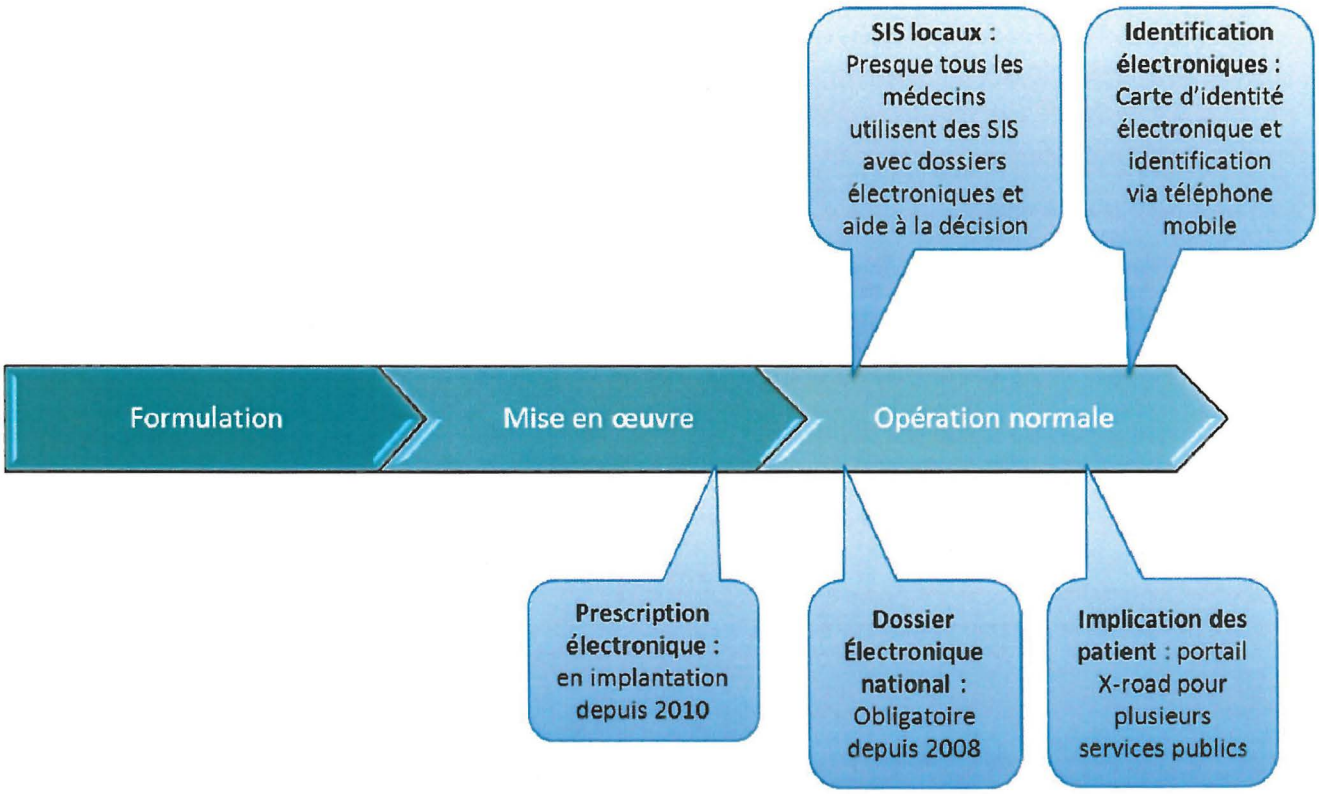
Estonie	
Population	**1 335 347**
Espérance de vie	**75 ans**
Nombre de médecins (par 1 000 hab.)	**3,3**
Nombre de lits d'hôpital (par 1 000 hab.)	**5,4**
Dépenses de santé (par habitant, $US PPP)	**1393**
Dépenses de santé (en % du PIB)	**7%**
Part du financement public	**75,3%**

La santé électronique en Estonie

L'Estonie est un des pays les plus avancés en termes d'informatisation de la santé. Ce projet fait d'ailleurs partie d'une volonté de s'en aller vers des services publics de plus en plus informatisés, comme on peut le voir sur le portail Internet X-road, qui permet aux citoyens d'accéder aux services de santé mais aussi entre autres de taxation, des outils d'éducation, de police ou encore de vote électronique.

Cet avancement dans l'application des nouvelles technologies dans les services publics est essentiellement soutenu par un système d'authentification par les cartes d'identité électroniques mises en circulation depuis 2002 et l'identification via les téléphones mobiles depuis 2007.

Figure 6 : L'avancement des projets d'informatisation de la santé en Estonie



Le Projet Santé Estonien 2015, lancé depuis 2000 par le ministère des affaires sociales (en charge de l'informatisation de la santé sauf la prescription électronique confiée au Fond d'Assurance Santé Estonien) a permis de lancer des projets d'envergure, si bien qu'aujourd'hui presque tous les médecins utilisent des SIS comprenant des dossiers électroniques, des EIOM pour les prescriptions électroniques et des systèmes d'aide à la décision ou de partages de données d'imagerie. Depuis 2005, c'est la Fondation Estonienne de Santé Électronique qui gère les projets d'envergure comme celui du dossier électronique national (2008) et de la prescription électronique à l'échelle du pays (2010).

Le dossier électronique national concerne tous les résidents, de la naissance au décès. Il est obligatoire pour les médecins d'y ajouter certaines informations concernant les épisodes de soin et les patients peuvent y ajouter des informations sur leur souhaits concernant le don d'organes ou la réanimation. Ce système a été développé par l'État.

Les réactions face aux risques en Estonie

On ne trouve pas en Estonie un seul document regroupant toute la stratégie sur l'informatisation de la santé : on a plusieurs initiatives sur la santé électronique uniquement ainsi qu'une multitude d'autres sur la prestation électronique des services publics qui ont un volet santé.

La principale loi portant sur l'informatique de santé est la Loi sur l'Organisation des Services de Santé et surtout ses amendements votés en 2007, qui gèrent la sécurité et la disponibilité des données en renvoyant à la Loi sur la Protection des Données Personnelles de 2001. Ces deux lois reconnaissent que l'intégrité, la disponibilité et de la confidentialité des SIS sont centrales mais n'expliquent pas comment elles doivent être préservées.

Au niveau de la sécurité, les données de santé rentrent dans un système de protection des données plus large. Les informations issues de toutes les bases de données publiques sont cryptées, une grande prévention face aux attaques est faite. Le Département de Protection des Infrastructures de Données Critiques évalue la sécurité des systèmes d'information et propose des conseils pour protéger les informations vitales. L'Équipe de Réponse aux Urgences Informatiques, s'occupe des éventuels incidents et peut être assistée si besoin de la Ligue de CyberDéfense. Cette expertise est internationalement reconnue puisque le centre de compétences des Nations Unies sur la CyberDéfense se trouve en Estonie.

Selon la loi, la création d'un dossier électronique est effective à moins que le patient le refuse («opt-out system»). Les professionnels ont ensuite accès aux dossiers des patients, mais ceux-ci peuvent retirer l'accès à certains professionnels. Tous ces accès sont enregistrés et le patient peut vérifier qui a accédé à ses données. En effet, un professionnel de santé n'est sensé consulter les dossiers que des patients dont il s'occupe («attending doctor concept»).

On peut donc dire que la sécurité face aux accès extérieurs est assez forte, mais c'est à l'interne que les problèmes de posent. Certains disent qu'il est facile de cacher ses traces dans l'accès au dossier d'un patient, et c'est à ce dernier de vérifier si les personnes qui ont consulté son dossier sont les bonnes. Plusieurs acteurs en Estonie seraient favorables à une nouvelle loi pour gérer les mauvaises utilisations potentielles.

Enfin, certains médecins expriment quelques doutes face aux SIS, alors qu'ils sont souvent les premiers supporteurs de ce genre de projets. Ils sont inquiets du fait qu'ils ne reçoivent pas assez de formation pour utiliser les outils informatiques, ce qui rend certains médecins incapables d'utiliser correctement les SIS, surtout au niveau de la prescription électronique, alors qu'ils y sont obligés.

Sources: (European Commision, 2010), (Health Policy Monitor, 2010), (Estonian ICT Export Cluster, 2012)

La France

Tableau 4 : Informations sur la santé en France (OCDE, 2011)

France	
Population	**62 747 780**
Espérance de vie	**81 ans**
Nombre de médecins (par 1 000 hab.)	**3,3**
Nombre de lits d'hôpital (par 1 000 hab.)	**6,6**
Dépenses de santé (par habitant, $US PPP)	**3978**
Dépenses de santé (en % du PIB)	**11,8%**
Part du financement public	**77,9%**

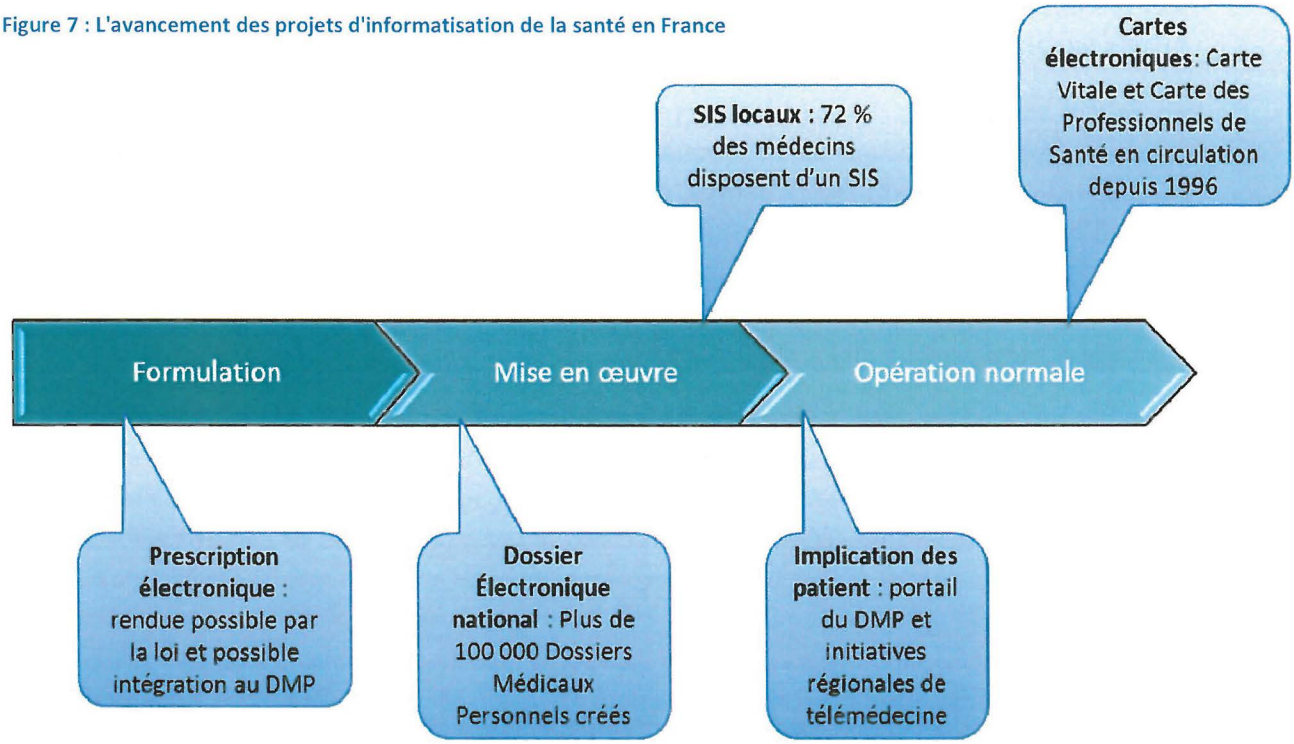
La santé électronique en France

Comme le montre la Figure 4, les différents projets d'informatisation de la santé en France en sont à des stades d'avancement très différents. Certaines fonctionnalités sont implantées depuis longtemps comme le système des cartes électroniques pour les patients (Carte Vitale) et pour les professionnels (Carte des Professionnels de la Santé), mais ces dernières sont plutôt liées au système de remboursement.

Chez les médecins, l'utilisation d'un SIS est en augmentation avec notamment un très bon score au niveau du partage de données radiologiques. Dans ces SIS, on parle le plus souvent de gestion locale des dossiers puisque l'aide à la décision et la prescription électronique ne sont pas encore répandus. Ces systèmes ne sont pas encore très reliés, mais ceci est en train de changer avec l'implantation du système national qu'est le Dossier Médical Personnel (DMP).

Officiellement annoncé en 2004 mais vraiment relancé en 2009, le DMP est un dossier longitudinal de niveau national sur les patients. Chaque intervenant de la santé s'il est autorisé peut accéder aux renseignements nécessaires à la prestation des soins et y ajouter des informations pertinentes sur les épisodes de traitement du patient. Ce dernier peut aussi y entrer ses vœux sur le don d'organes ou encore la réanimation. La prescription électronique, bien que discutée et rendue légalement possible, ne fait pas encore partie de ce système.

Figure 7 : L'avancement des projets d'informatisation de la santé en France



Les patients ont un accès total à leur DMP via le portail dmp.gouv.fr qui fonctionne depuis 2011. On peut enfin relever les différentes initiatives de télésanté en France lancées par les grands hôpitaux et de plus en plus nombreuses mais qui restent encore la plupart du temps de niveau local.

Les réactions face aux risques en France

Depuis septembre 2009, la gestion des activités de santé électronique a été pour la majeure partie transférée à une agence directement reliée au Ministère de la Santé et des Sports : l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé). La prise de décision stratégique reste au niveau du ministère au sein de sa direction de la stratégie des systèmes d'Information de Santé.

Le choix en matière de SIS locaux est laissé à la discrétion des professionnels, mais certaines règles s'appliquent. L'ASIP Santé a notamment la responsabilité de faire passer un agrément aux

hébergeurs de données de santé. Ces derniers, doivent se conformer à un certain nombre de normes notamment de sécurité qu'ils s'agissent d'entreprises spécialisées, de concepteurs de logiciels ou bien d'une organisation de santé qui stocke ses propres données et qui souhaite se relier à un système plus large.

En ce qui concerne les SIS qui permettent l'EIOM, une toute nouvelle homologation est disponible depuis peu. Dirigée par la Haute Autorité de Santé, qui est une organisation publique indépendante, cette certification permet de s'assurer du respect de certaines normes de sécurité et de qualité dans un système d'EIOM. Pour l'instant cette charge a été confiée à la firme SGS, et les logiciels destinés aux hôpitaux et aux services ambulanciers sont visés. L'homologation n'a pas un caractère obligatoire pour l'instant mais se place plutôt comme un avantage stratégique pour les logiciels approuvés.

En ce qui concerne les règles sur les différents accès au DMP, on retrouve cela à la fois dans le décret sur la confidentialité 2007-960 du code de la santé publique et dans la loi sur la protection des données. Le premier droit reconnu est celui pour les patients d'accéder à toutes leurs données, ce qui est possible via le site Internet du DMP. Par ce biais, ils peuvent gérer les droits d'accès à leur dossier puisque chaque accès au DMP doit être consenti. Une exception est faite pour les cas d'urgence où on considère que l'accès est consenti à moins que le patient ne l'ait explicitement spécifié auparavant. Chaque patient pourra vérifier les accès à son DMP, puisque toute entrée est enregistrée, avec le nom de la personne et la date. Pour authentifier les accès, on se sert des deux systèmes de cartes : la Carte Vitale et la CPS.

Enfin, l'ASIP Santé annonce qu'une nouvelle politique générale de sécurité des systèmes d'information de santé (PGSSI-Santé) est en préparation, présentement la phase de consultation est en cours et on prévoit sa publication pour 2013.

Sources : (European Commission, 2010), (ASIP Santé, 2012a), (ASIP Santé , 2012b), (HAS, 2012)

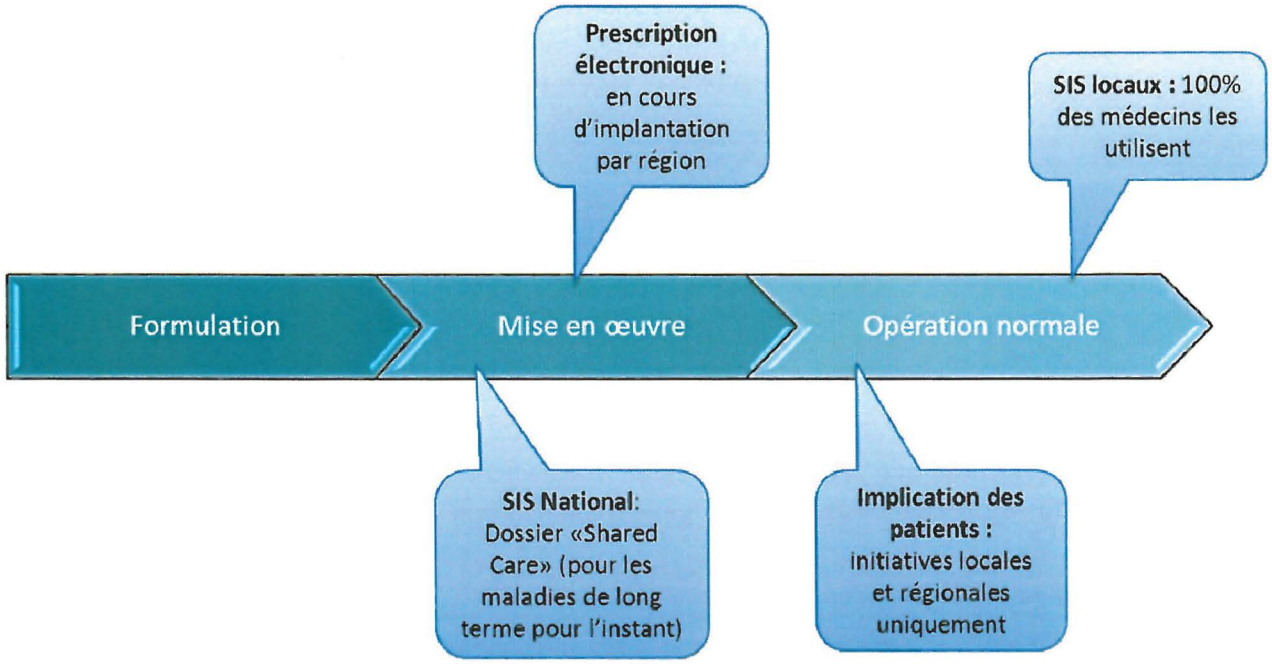
La Nouvelle Zélande

Tableau 5 : Informations sur la santé en Nouvelle Zélande (OCDE, 2011)

Nouvelle Zélande	
Population	**4 291 900**
Espérance de vie	**80,8 ans**
Nombre de médecins (par 1 000 hab.)	**2,6**
Nombre de lits d'hôpital (par 1 000 hab.)	**2,3**
Dépenses de santé (par habitant, $US PPP)	**2983**
Dépenses de santé (en % du PIB)	**10,3%**
Part du financement public	**80,5%**

La santé électronique en Nouvelle Zélande

Figure 8 : L'avancement des projets d'informatisation de la santé en Nouvelle Zélande



La Nouvelle Zélande est reconnue pour son avancement dans le domaine de l'informatisation de la santé. En effet, l'ensemble des professionnels de la santé en fait usage autant dans les cabinets médicaux que dans les hôpitaux. Pourtant, le point faible de ce système bien implanté réside dans le fait que ces SIS locaux sont très peu reliés entre eux et que l'interconnexion n'est pas encore vraiment rentrée dans les mœurs.

Dans leur plan «National Health IT Plan» de septembre 2010, le National Health IT Board, organisme encadrant l'informatique de santé, entend mettre en place des stratégies de connexion entre les SIS locaux. Il souhaite la mise en place d'un dossier national appelé «Shared Care» pour l'ensemble de la population. Pour l'instant, celui-ci est en phase d'implantation et s'applique uniquement aux personnes souffrant d'une condition à long terme.

Ce dossier médical national est assez unique, du fait qu'il contient deux parties : une sur le passé (cela comprend les antécédents médicaux de la personne, ses épisodes de soin) mais aussi une partie sur le futur, où le patient et souvent sa famille (Whanau) se réunit avec le médecin pour constituer une sorte de plan de soins concerté, ce qui se révèle très utile pour les maladies chroniques notamment. Le système Shared Care possède aussi un plan d'aide à la décision pour les médecins.

Une autre initiative d'interconnexion entre les différents professionnels de santé via leurs SIS est le service de prescription électronique, qui est en train d'être implanté nationalement après des projets pilotes régionaux. Ce système fonctionne à l'aide d'un code à barres, donné au patient par le médecin prescripteur. Pour récupérer ses médicaments, le patient n'a qu'à donner son code à barre à une pharmacie qui va pouvoir télécharger la prescription stockée sur une base de données commune. Il n'y a plus de retranscription de prescription à faire et les médecins peuvent être informés si leur patient est allé chercher ses médicaments ou non.

Les réactions face aux risques en Nouvelle-Zélande

En Nouvelle-Zélande, un peu comme au Danemark, les SIS se sont d'abord développés sans que la législation qui l'entoure ne soit trop pesante. Aucune réglementation au niveau national n'avait été prise, d'autant plus que la gouvernance autour de l'informatisation de la santé était plus régionale que nationale. On note simplement que la loi règlemente l'usage et la confidentialité des informations de santé (Health Information Privacy Code de 1993). On le voit bien dans l'initiative Shared Care, ou un certain nombre de règles de confidentialité sont clairement définis et dépendent de ces lois.

La Nouvelle-Zélande est désormais arrivée à un tournant puisque depuis quelques années, elle cherche à uniformiser toutes ces initiatives, et cela concerne aussi les différents risques posés

par les SIS. L'organisme qui prend les devants dans cette tendance est le HISO (Health Information Standards Organisation), qui a déjà rédigé une sorte de guide de sécurité pour l'informatique de santé qui va s'appliquer à l'ensemble du secteur (HISO 10029.1). HISO met aussi en place des listes de critères de certification pour faire un choix de SIS dans le cadre de certains programmes nationaux comme l'initiative Connected Health. Ce programme, qui a pour but de mettre en place une interface permettant de lier tous les SIS auxquels un médecin se connecte pour éviter toute sorte de confusion, est désormais réalisé par un certain nombre de systèmes, qui ont dû être certifiés en remplissant les critères cités par HISO.

Cette évolution touche aussi les dossiers locaux, pour lesquels on envisage de mettre en place une liste d'exigences communes. Cette volonté, notamment rendue publique par un document rédigé par Patient Firsts, qui représente les associations de médecins, envisage plusieurs possibilités de certifications comme de passer par des firmes sous contrats pour donner une accréditation, comme cela se fait par exemple aux États-Unis.

Sources: (HISO, 2012), (Patient First, 2011), (National Health IT Board, 2010), (IT health board, 2012)

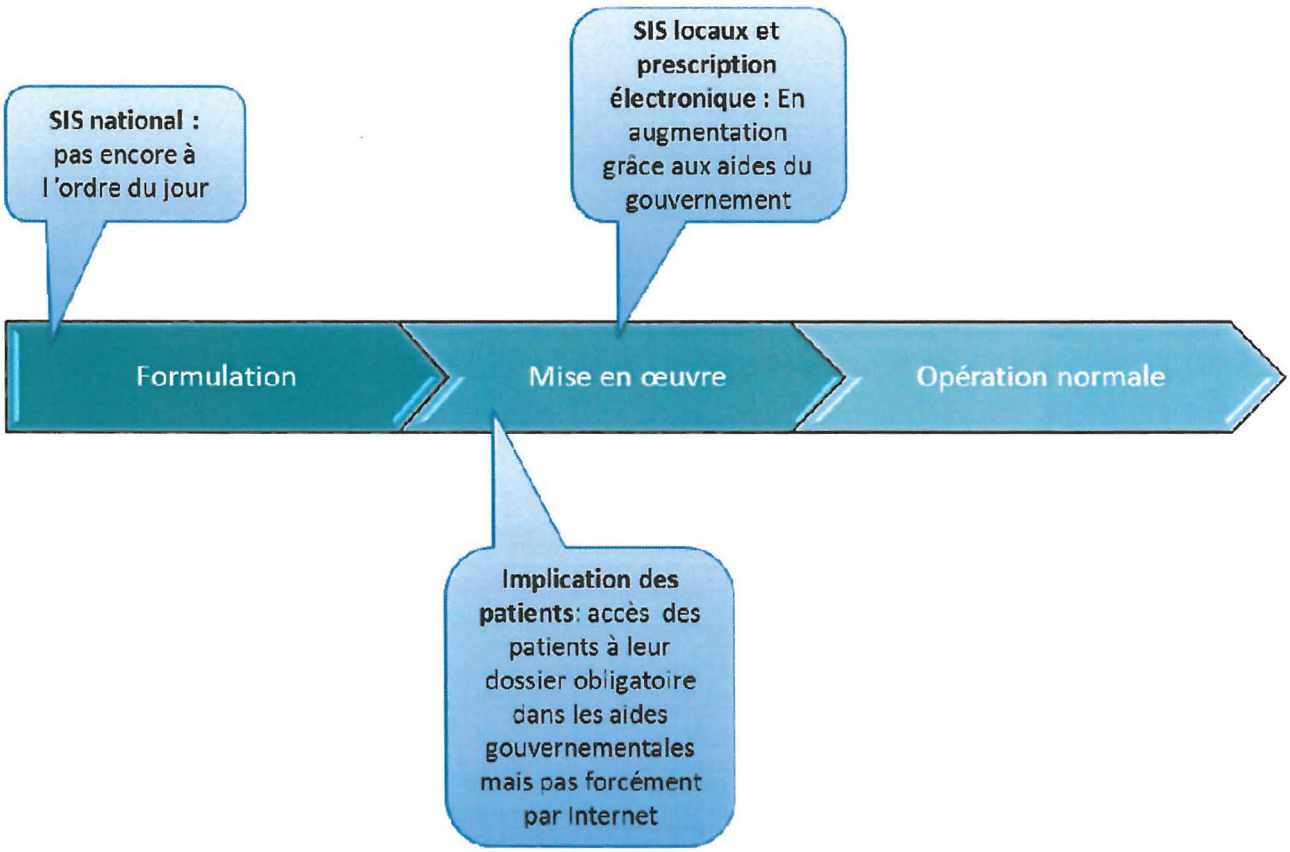
Les États-Unis

Tableau 6 : Informations sur la santé aux États-Unis (OCDE, 2011)

Etats-Unis	
Population	**313 232 000**
Espérance de vie	**78,2 ans**
Nombre de médecins (par 1 000 hab.)	**2,4**
Nombre de lits d'hôpital (par 1 000 hab.)	**3,1**
Dépenses de santé (par habitant, $US PPP)	**7960**
Dépenses de santé (en % du PIB)	**17,4%**
Part du financement public	**47,7%**

La santé électronique aux États-Unis

Figure 9 : L'avancement des projets d'informatisation de la santé aux États-Unis



Aux États-Unis, l'informatisation de la santé est bien moins avancée qu'elle peut l'être dans d'autres pays. En 2011, si on dénombre que 50% des médecins possèdent un SIS, ils ne sont à peine plus de 10% à en utiliser les pleines fonctionnalités. Du côté des hôpitaux, le bilan n'est guère plus positif, puisque seulement 11.9% des hôpitaux utilisent un SIS. En réalité, certains groupes régionaux à l'échelle de grandes villes ou de regroupements locaux sont très avancés mais ils restent une minorité.

Face à ce constat, l'administration Obama a décidé de donner un vrai élan à l'informatisation de la santé, en étant convaincue que celle-ci pourra augmenter l'efficacité des soins. Dans le cadre de l'ARRA (American Recovery and Reinvestment Act) est passé la loi HITECH (Health Information Technology for Economic and Clinical Health) qui va dans le sens d'une forte adoption des SIS par les professionnels de santé.

La loi HITECH propose des sommes aux professionnels qui s'équipent de SIS et qui répondent à certains critères de bonne pratique appelés «Meaningful Use». Ces incitations économiques ont été proposées dans le but d'amener à une utilisation majoritaire des SIS d'ici 2014, mais les différents critères que doivent remplir les professionnels de santé ne sont pas directement décrits dans la loi HITECH. C'est le ministère de la Santé et des Services à la Personne qui publie les critères de Meaningful Use, la première étape a d'ailleurs été rendue publique en juillet 2010 et d'autres étapes assorties d'autres critères suivront.

Les réactions face aux risques aux États-Unis

C'est la HIPAA (Health Insurance Portability and Accountability Act) qui régit la confidentialité des informations contenues dans les SIS. Cette loi définit les informations devant être utilisées avec précaution et attention : ce sont les PHI (Protected Health Information).

Plusieurs mesures entourant les risques liés au SIS sont comprises dans les critères de Meaningful Use. On peut tout d'abord relever que le choix des professionnels de santé se fait parmi un ensemble de SIS certifiés. Cette certification est la responsabilité de l'ONC (Office of the National Coordinator for health information technology), mais elle délègue ensuite à des organisations sélectionnées le droit d'accorder les homologations aux vendeurs de SIS.

Au sein des critères pour la première étape du programme on trouve une obligation de protéger les PHI (Protected Health Information), et ceci est contrôlé par une sorte d'audit pour s'assurer que le SIS est utilisé dans les cadres de la HIPAA. Le propriétaire du SIS a ensuite le devoir d'effectuer les modifications qui sont recommandées d'après l'analyse de sécurité. Cette dernière peut être effectuée à l'interne si le personnel est formé adéquatement, ou par des firmes de conseil. On peut remarquer qu'en plus de mesures techniques, l'analyse permet aussi de voir si le personnel est suffisamment formé à l'utilisation du SIS.

Un autre critère est celui de donner accès au patient à une copie électronique de son dossier s'il le demande. Le patient à le droit de consulter son dossier mais il n'y a pas encore de possibilité de le faire de façon systématique (comme via un portail Internet).

De plus, la confidentialité des données est prise au sérieux. Tout bris qui concerne plus de 500 patients doit être divulgué publiquement. Par contre malgré cette mesure qui crée un «wall of shame» autour des organisations qui n'ont pas pu garantir la confidentialité des PHI, on dénombre quand même encore beaucoup de bris de confidentialité, et plus particulièrement effectués au sein même des organisations médicales, par curiosité ou pour la revente d'informations d'assurance pour permettre des soins gratuits.

Enfin, si on ne voit pas de mesure phare en ce qui concerne les risques liés à l'intégration du SIS, ceux-ci commencent à être rendus publics, bien que peu documentés exactement. Ils ont fait cette année, l'objet d'un rapport de l'IOM (Institute of Medicine) commandé par le ministère de la Santé et des Services à la Personne, et de nombreuses recommandations ont été formulées.

Sources: (Institute of Medicine, 2012), (Collier, 2012), (Health Policy Monitor, 2010), (Office of the National Coordinator for Health Information Technology, 2012), (American National Standards Institute, 2012)