Agence de la santé
et des services sociaux
de l'Estrie
Québec

Politique sur la sécurité des actifs informationnels

Version 1

Direction des ressources financières, informationnelles et matérielles
Septembre 2006

Adoptée par le conseil d'administration de l'Agence de l'Estrie le 25 octobre 2006.

TABLE DES MATIÈRES

Contexte

L'apport grandissant des technologies de l'information à la prestation des services, l'échange d'information nécessaire au fonctionnement en réseaux intégrés de services et la création du Réseau de télécommunication sociosanitaire (RTSS) ont entraîné des modifications majeures dans les caractéristiques du réseau sociosanitaire. L'échange d'information est maintenant au cœur de l'organisation des services et bien que la clientèle en soit avantagée, il devient impératif que cela se fasse dans le plus grand respect des lois et exigences en cette matière et en conformité avec les valeurs et les principes associés à la protection de la vie privée. À cet effet, le ministère de la Santé et des Services sociaux (MSSS) a élaboré un cadre global de gestion des actifs informationnels appartenant aux organismes du réseau[1] dans lequel il précise ses exigences en cette matière.

L'Agence de la santé et des services sociaux de l'Estrie (l'Agence) reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. L'Agence reconnaît détenir, en outre, des renseignements personnels très sensibles entre autres par l'entremise des services informationnels qu'elle offre et qui ont une portée régionale ainsi que des informations qui ont une valeur légale, administrative ou économique.

C'est dans cette optique que l'Agence met en place la présente politique de sécurité de l'information qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information. La démarche vise donc à assurer l'intégrité, la confidentialité et la continuité des informations et la présente politique constitue l'élément de base.

Dans le présent document, le terme « utilisateur, utilisatrice » désigne les employés et employées, les médecins, le personnel professionnel, les bénévoles, les stagiaires, les chercheurs et chercheuses ainsi que les consultants et consultantes.

1. QUÉBEC (GOUVERNEMENT), MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX. *Cadre global de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux – Volet sur la sécurité*, Québec, septembre 2000, 76 p.

1. Objectifs de la politique

La politique vise à assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications. Plus spécifiquement, les objectifs de l'Agence en matière de sécurité de l'information sont :

- assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs à la clientèle et au personnel de l'Agence;

- assurer la disponibilité, l'intégrité et la confidentialité de l'information et ce, tant à l'égard de l'utilisation des systèmes et réseaux informatiques, des télécommunications, de l'Internet, des actifs informationnels et de tout autre système d'information contenant des données corporatives, peu importe le support sur lequel elles sont consignées ou conservées;

- assurer la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations régionales.

Cette politique sera suivie de directives, normes et procédures qui viendront préciser les obligations qui en découlent.

2. Respect de la politique

Le président-directeur général de l'Agence nomme une personne responsable de la sécurité des actifs informationnels (RSAI) qui est chargée de l'application de la présente politique.

L'Agence exige de l'utilisateur ou de l'utilisatrice qui accède aux actifs informationnels internes, ainsi qu'aux actifs régionaux qui y sont hébergés, de se conformer aux dispositions de la présente politique ainsi qu'aux normes, directives et procédures qui s'y rattachent.

Afin de s'assurer du respect de la présente politique, l'Agence peut surveiller, contrôler, vérifier et enregistrer tout accès, toute session, connexion, utilisation, communication ou échange faits sur les actifs informationnels et à l'aide de ceux-ci.

Le non-respect de la politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement, et ce, conformément aux dispositions des conventions collectives.

3. Portée

La présente politique s'applique :

- à tout utilisateur ou utilisatrice, personne physique ou morale, qui utilise ou qui accède pour le compte de l'Agence à des informations confidentielles, nominatives ou corporatives, quel que soit le support sur lequel elles sont conservées, échangées ou véhiculées;

- à tout utilisateur ou utilisatrice, personne physique ou morale, qui utilise ou qui accède à un système informationnel à portée régionale, pour le compte d'un établissement du réseau de la santé et des services sociaux, à des informations confidentielles, nominatives ou corporatives, quel que soit le support sur lequel elles sont conservées, échangées ou véhiculées;

- à l'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein de l'Agence, tels que les banques d'information électronique, les informations et les données sans égard aux supports (incluant le support papier), les réseaux, les systèmes d'information, les systèmes téléphoniques et de communication, les logiciels et les équipements informatiques dont l'Agence est propriétaire, locataire ou fiduciaire;

- à l'ensemble des activités de collecte, d'enregistrement, de traitement, de communication, d'échange et de diffusion des données, d'entreposage, d'archivage et de destruction des données;

- à l'ensemble des actifs informationnels à connotation régionale localisés dans la salle des serveurs du Technocentre régional ainsi qu'à leur utilisation au sein d'un établissement, tels que les banques d'information électronique, les informations et les données sans égard aux supports (incluant le support papier), les réseaux, les systèmes d'information, les logiciels et les équipements informatiques dont l'Agence est propriétaire, locataire ou fiduciaire.

4. Principes directeurs

a. Tout utilisateur ou utilisatrice, ayant accès aux actifs informationnels internes à l'Agence comme aux actifs régionaux, assume par le fait même des responsabilités spécifiques en matière de sécurité et est redevable de ses actions auprès du président-directeur général de l'Agence.

b. L'Agence met à la disposition des utilisateurs et utilisatrices des outils de gestion et d'échange d'information qui doivent être utilisés à des fins professionnelles seulement et uniquement à l'exercice de leurs fonctions.

c. L’Agence met en place des mesures de protection, de prévention, de détection, d’assurance et de correction qui permettent d'assurer la confidentialité, l’intégrité, la disponibilité, l'authentification et l'irrévocabilité des actifs informationnels de même que la continuité des activités. Les mesures doivent notamment empêcher les accidents, l'erreur, la malveillance, l’indiscrétion ou la destruction d’information sans autorisation.

d. Afin de s’assurer d’une utilisation adéquate des actifs informationnels et d’autres outils de communication, l’Agence peut surveiller, contrôler, vérifier et enregistrer tout accès, utilisation, communication ou échange fait par les utilisateurs et les utilisatrices sur les actifs informationnels et à l’aide de ceux-ci.

e. Tout utilisateur ou utilisatrice est responsable des actions résultant de l’usage de ses clés d’accès, de son identifiant, de son code d’accès et de son mot de passe. L’utilisateur ou l’utilisatrice peut être redevable des actes qui ont été posés à l’aide de ceux-ci.

   Le personnel doit obligatoirement suivre un programme de sensibilisation et de formation à la sécurité informationnelle et à la confidentialité mis en place à son intention. Au terme de cette formation, le personnel signe un engagement au respect de la confidentialité et à la protection des renseignements personnels.

f. Les renseignements personnels doivent être utilisés et ne servir qu’aux fins pour lesquelles ils ont été recueillis ou obtenus. Toute collecte, transmission, échange ou communication d’information nominative doit se faire dans le respect des lois en cette matière et des exigences découlant de normes, directives et procédures mises en application par l’Agence.

g. L'accès aux renseignements personnels de la clientèle et du personnel peut être contrôlé et journalisé. Chaque système doit prévoir des mécanismes permettant d’accorder des droits d'accès différents selon les catégories de personnel et de vérifier toutes les actions posées sur les données sensibles.

h. Le droit d’accès aux actifs informationnels est attribué en fonction de ce qui est strictement nécessaire pour l’exécution des tâches à accomplir. Cette règle s’applique également au personnel de soutien informatique.

i. Les ententes et contrats liés à l’Agence doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l’information.

j. L’Agence, par son Technocentre régional, élabore et applique des normes reconnues en matière de gestion des systèmes d’information, principalement en regard de la disponibilité et de la confidentialité. Le respect de ces normes primera dans l’offre de service et pourra exiger des actions particulières de la part des utilisateurs et utilisatrices.

5. Rôles et responsabilités

5.1. Le conseil d'administration de l'Agence

Comme le prévoit le Cadre global, le conseil d'administration approuve la présente politique et mandate le président-directeur général pour sa mise en œuvre. De plus, le conseil d'administration doit effectuer les suivis concernant l'application de la politique et doit également approuver le bilan annuel concernant cette dernière.

5.2. Le président-directeur général

Le président-directeur général est le premier responsable de la sécurité des actifs informationnels au sein de l'Agence. Il s'assure que les valeurs et les orientations en matière de sécurité soient partagées par l'ensemble des gestionnaires, des utilisateurs et utilisatrices de l'Agence ainsi que des utilisateurs et utilisatrices de services régionaux qui se trouvent à l'Agence. À cette fin, il s'assure de l'application de la politique dans l'organisation, apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique, soumet le bilan annuel concernant l'application de la politique au conseil d'administration, exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

Le président-directeur général doit s'assurer que toutes les données à caractère nominatif obtenues par la DSPE, dans le cadre de la Loi sur la santé publique, sont conservées sous l'autorité du directeur ou de la directrice de santé publique et de l'évaluation, séparément des autres données détenues par les autres directions de l'Agence et que les personnes ayant accès à ces renseignements, pour l'exercice de leurs fonctions, s'engagent sous serment à ne pas les divulguer ou les communiquer sans y être dûment autorisées.

Pour le représenter en cette matière dans l'organisation et pour la réalisation de l'ensemble des mesures précitées, il a nommé la personne responsable de la sécurité des actifs informationnels.

5.3. La personne responsable de la sécurité des actifs informationnels (RSAI)

À titre de représentante déléguée du président-directeur général en matière de sécurité des actifs informationnels, la personne RSAI gère et coordonne la sécurité au sein de l'Agence. Elle doit donc harmoniser l'action des divers acteurs et actrices dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité de l'information. Cette responsabilité exige une vision globale de la sécurité au sein de l'Agence.

La personne RSAI veille à l'élaboration de la politique sur la sécurité et à son application une fois adoptée par l'Agence. Dans cette perspective, la personne RSAI collabore avec tous les gestionnaires et, en particulier, avec la ou le gestionnaire chargé des technologies de l'information. Plus précisément, la personne RSAI :

- élabore la politique sur la sécurité des actifs informationnels, la soumet à différentes instances pour adoption. Elle la remet ensuite au président-directeur général qui la présente au conseil d'administration pour approbation;

- met en place et préside le comité de protection des renseignements personnels et de sécurité des actifs informationnels, qui pourra être formé des détenteurs ou détentrices d'actifs informationnels, d'une ressource informatique ou de la personne responsable de la protection des renseignements personnels et de représentants ou représentantes des ressources humaines, financières et matérielles;

- coordonne, avec les secteurs visés et en concordance avec les orientations régionales, la mise en oeuvre de la politique sur la sécurité adoptée par l'organisme et en suit l'évolution;

- identifie les risques auxquels sont soumis les actifs et propose des mesures pour les réduire en collaboration avec les gestionnaires et les détenteurs et détentrices d'actifs informationnels;

- s'informe des besoins en matière de sécurité auprès des détenteurs, des détentrices et des gestionnaires, leur propose des solutions et coordonne la mise en place de ces solutions;

- gère les aspects relatifs à l'escalade des incidents de sécurité à l'échelle locale et procède à des évaluations de la situation en matière de sécurité;

- suit la mise en oeuvre de toutes recommandations découlant d'une vérification ou d'un audit;

- produit annuellement, et au besoin, les bilans et les rapports relatifs à la sécurité des actifs informationnels appartenant à l'Agence en s'assurant que l'information sensible à diffusion restreinte est traitée de manière confidentielle. Elle s'assure également de transmettre le bilan annuel au coordonnateur régional de la sécurité des actifs informationnels.

5.4. Les détenteurs et détentrices d'actifs informationnels

Les détenteurs et détentrices :

- déterminent les règles d'accès et autorisent les accès aux actifs dont ils ou elles assument la responsabilité avec l'appui du RSAI de l'organisme;

- assurent la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés légalement par le Cadre global ou le président-directeur général;

- s'impliquent dans l'ensemble des activités relatives à la sécurité, notamment l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques et, finalement, la prise en charge des risques résiduels;

- s'assurent que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement en plus de s'assurer que leur nom et la liste des actifs dont ils ou elles assument la responsabilité soient consignés dans le registre des autorités.

5.5. La personne responsable de la protection des renseignements personnels (RPRP)

À titre de responsable de l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la personne RPRP a un rôle conseil auprès de la personne RSAI afin de s'assurer que les mécanismes de sécurité mis en place permettent de respecter les exigences de cette loi. Cette responsabilité se manifeste aussi dès le début du développement d'un nouveau système où la personne RPRP doit introduire les préoccupations et les exigences relatives à la protection des renseignements nominatifs.

5.6. Le professionnel ou la professionnelle en sécurité de l'information (PSI)

Le rôle du professionnel ou de la professionnelle de la sécurité de l'information est de conseiller la personne RSAI sur les aspects technologiques et méthodologiques concernant la sécurité. Cette personne coordonne les travaux reliés à l'implantation et aux contrôles des mesures de sécurité. Elle coordonne ou réalise les tâches de sécurité opérationnelles qui lui sont confiées par la personne RSAI.

5.7. Le chef des ressources informationnelles

Le rôle du chef et de son service des ressources informationnelles à l'égard de la sécurité de l'information est d'agir en tant que fournisseur de services. Il fournit et maintient en état les moyens techniques de sécurité et s'assure de leur conformité aux besoins de sécurité déterminés par les détenteurs et détentrices. Ce rôle trouve son complément dans l'assistance et le conseil en vue d'une meilleure utilisation de ces moyens.

5.8. Les gestionnaires

Les gestionnaires s'assurent que tout leur personnel, incluant les nouveaux employés et employées, sont au fait de leurs obligations découlant de la présente politique. Ils les informent de l'existence de la politique sur la sécurité des actifs informationnels à l'Agence et plus précisément sur les normes, directives et procédures de sécurité en vigueur. Les gestionnaires doivent également présenter et faire compléter le formulaire d'engagement à la confidentialité à tout nouvel employé ou employée.

Les gestionnaires informent et sensibilisent les utilisateurs et utilisatrices à l'importance des enjeux de sécurité. Ils doivent s'assurer que les moyens de sécurité sont utilisés de façon à protéger effectivement l'information utilisée par les utilisateurs et utilisatrices.

Ils communiquent à la personne RSAI tout problème d'importance en matière de sécurité de l'information.

5.9. Les utilisateurs et utilisatrices

Chaque utilisateur ou utilisatrice des actifs informationnels assume par le fait même des responsabilités spécifiques en matière de sécurité et est redevable de ses actions auprès des dirigeants de l'Agence. L'utilisateur ou l'utilisatrice est notamment responsable de l'application et du respect des normes, directives et procédures en vigueur en matière de sécurité de l'information. Cette personne doit également informer son gestionnaire de toute violation des mesures de sécurité dont elle pourrait être témoin ou de toute anomalie décelée pouvant nuire à la sécurité des actifs informationnels.

ANNEXE 1 – LEXIQUE

- **Actif informationnel :** Banque d'information électronique, système d'information, réseau de télécommunications, technologie de l'information, installation ou ensemble de ces éléments; un équipement médical spécialisé ou ultraspécialisé peut comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels. (Loi sur les services de santé et les services sociaux, art. 520.1). S'ajoutent, dans le présent cadre de gestion, tout document ou dossier papier ou encore document imprimé généré par les technologies de l'information.

- **Agence :** Agence de la santé et des services sociaux de l'Estrie.

- **Authentification :** Fonction permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

- **Banque d'information électronique :** Base de données dont l'usage n'est possible qu'avec des technologies de l'information.

- **Confidentialité :** Propriété d'une information d'être accessible aux seuls utilisateurs et utilisatrices autorisés.

- **Détenteur, détentrice :** Personne à qui, par délégation du sous-ministre ou d'un dirigeant d'organisme, est assignée la responsabilité d'assurer la sécurité d'un ou de plusieurs actifs informationnels, qu'ils soient détenus par le sous-ministre, un dirigeant d'organisme ou un tiers mandaté.

- **Disponibilité :** Propriété d'une information d'être accessible et utilisable en temps voulu et de la manière adéquate par un utilisateur ou une utilisatrice autorisée.

- **Intégrité :** Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

- **Irrévocabilité:** Propriété d'un acte d'être définitif et clairement attribué à la personne qui l'a accompli ou au dispositif avec lequel cet acte a été accompli.

- **Renseignement confidentiel :** Tout renseignement qui ne peut être communiqué ou rendu accessible qu'aux utilisateurs ou utilisatrices ou autres entités autorisées.

- **Renseignement personnel ou nominatif :** Tout renseignement qui concerne une personne physique et qui permet de l'identifier.

- **Réseau informatique :** Ensemble des composantes et des équipements informatiques reliés par voie de télécommunications, soit pour accéder à des ressources ou à des services informatisés, soit pour en partager l'accès.

Annexe 2 – Fondement juridique

- Charte des droits et libertés de la personne (L.R.Q., c.C-12)
- Charte canadienne des droits et libertés (L.R.C., 1985, ch 11)
- Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2)
- Loi sur la santé publique (L.R.Q., c. S-2.2)
- Loi sur les archives (L.R.Q., c. A-21.1)
- Loi sur l'accès aux documents des établissements publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)
- Loi sur l'administration publique (L.R.Q., c. A-6.01)
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1)
- Certaines dispositions pertinentes du Code civil du Québec (C.C.Q.)
- Certains articles du code criminel du Canada (L.R.C., 1985, ch C-46)
- Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch.5)
- Loi canadienne sur le droit d'auteur (L.R.C. 1985, ch. C-42)
- Loi sur la propriété intellectuelle et les marques de commerce (L.R.C. 1985 ch. T-13)
- Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité (ministère de la Santé et des Services sociaux, septembre 2002)
- Architecture gouvernementale de la sécurité de l'information (septembre 2001)