Régie de l'assurance maladie Québec

POLITIQUE
RI-1202

IDENTIFICATION DU DOCUMENT
Section obligatoire

Titre	Sécurité de l'information	Date d'entrée en vigueur	2014-06-19
Thème	Ressources informationnelles		
Sous-thème	Protection et sécurité de l'information		
Unité responsable	Direction de la planification, de l'intégration, des architectures et de la sécurité		
Adoptée par	Président-directeur général	Date d'adoption	2016-05-05

Original signé par Jacques Cotton	2016-05-05
Signature du PDG	Date de la signature

INTRODUCTION
Section obligatoire

CONTEXTE

Afin de remplir adéquatement sa mission, la Régie collecte, produit, utilise, communique, échange, conserve et dispose d'information sous plusieurs formes. Cette information possède une valeur administrative, économique, légale et patrimoniale.

Le maintien de la qualité des services offerts par la Régie, sur laquelle repose la confiance de sa clientèle et de ses partenaires, nécessite l'implantation de mesures de sécurité à la hauteur de la valeur de l'information à protéger et des risques encourus.

En vertu de la Loi sur l'accès des documents des organismes publics et sur la protection des renseignements personnels, un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Par ailleurs, la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et entreprises du gouvernement établit les règles de gouvernance et de gestion en matière de ressources informationnelles applicables aux organismes publics et aux entreprises du gouvernement. Elle attribue notamment des responsabilités, en matière de sécurité de l'information, au dirigeant principal de l'information, au dirigeant réseau de l'information ainsi qu'au dirigeant sectoriel de l'information.

Enfin, la Directive sur la sécurité de l'information gouvernementale fixe les objectifs à atteindre, énonce les principes directeurs devant être appliqués et établit, notamment, les obligations des organismes publics pour assurer la sécurité de l'information gouvernementale tout au long de son cycle de vie.

CHAMP D'APPLICATION

Cette politique s'applique à toute information que détient la Régie ou dont elle a la gestion, notamment les banques confiées par le MSSS et le Dossier Santé Québec, et ce peu importe la forme, le support ou l'emplacement de cette information.

Cette politique s'adresse à l'ensemble du personnel de l'organisation et, plus particulièrement, aux gestionnaires responsables des unités administratives.

ÉNONCÉ DE LA POLITIQUE
Section obligatoire

OBJECTIFS

La présente politique vise à préciser les principes directeurs devant guider les actions de la Régie ainsi que ses relations d'affaires avec ses partenaires et ses fournisseurs en vue d'assurer la sécurité de l'information tout au long de son cycle de vie.

PRINCIPES DIRECTEURS

1. La sécurité de l'information se réalise en considérant :
   - les aspects humains, juridiques[1], organisationnels, opérationnels, technologiques et d'éthique de la gestion des actifs informationnels;
   - les champs d'intervention de la sécurité de l'information qui sont la prévention, la protection, la détection, l'intervention, le rétablissement et la correction;
   - les orientations et tendances qui se font valoir, dont les normes gouvernementales, nationales et internationales, et qui visent à maintenir une gestion performante et efficace de la sécurité.
2. Les décisions en matière de sécurité de l'information sont prises en tenant compte des objectifs stratégiques et opérationnels de la Régie.
3. La sécurité de l'information est un sujet qui interpelle l'ensemble du personnel de la Régie, ses partenaires et ses fournisseurs. Leur adhésion aux principes établis dans le cadre normatif[2] ainsi que leur respect des règles de sécurité mises en place constituent l'assise sur laquelle repose la sécurité de l'information.
4. Une saine gestion de la sécurité de l'information implique l'attribution de responsabilités clairement définies à tous les niveaux de l'organisation, une sensibilisation adéquate de toutes les parties et la mise en place d'un processus de gestion interne de la sécurité permettant, entre autres, l'application de sanctions en cas de non-respect des règles établies et une reddition de comptes adéquate.

[1] L'annexe 1 présente, à titre indicatif, les lois et règlements ayant un impact sur la gestion et l'application de la sécurité de l'information.

[2] L'annexe 2 présente, à titre indicatif, la structure du cadre normatif en matière de sécurité de l'information à la Régie.

5. La sécurité de l'information est prise en compte au moment de la conception, de la réalisation et de la modification des processus d'affaires et des moyens technologiques ou autres utilisés tout au cours du cycle de vie de cette information.
6. La planification et la mise en œuvre des actions en sécurité de l'information s'effectuent en tenant compte de :
   - la valeur, la nature, le contexte d'utilisation et l'ampleur de l'information concernée;
   - l'évaluation des risques à la sécurité de l'information, au regard de leur probabilité de réalisation ainsi que de leurs conséquences;
   - l'évaluation des coûts et bénéfices découlant de la mise en place des actions envisagées.
7. L'état de la sécurité de l'information est régulièrement vérifié et des plans d'actions sont constitués et mis en œuvre afin de corriger les vulnérabilités identifiées.
8. Tout événement ayant affecté ou mis en péril la sécurité de l'information doit être rapporté, répertorié et investigué. Au besoin, des mesures visant à corriger les déficiences constatées et à rétablir le niveau normal de sécurité sont appliquées dans des délais jugés raisonnables.

RÔLES ET RESPONSABILITÉS — Section obligatoire

Le président-directeur général (PDG)

Le PDG est le premier responsable de la sécurité de l'information détenue par la Régie. À ce titre, il voit à l'application des orientations gouvernementales et au respect des obligations légales et règlementaires.

Le dirigeant sectoriel de l'information (DSI)

Désigné par le PDG en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, le DSI veille à l'application des règles de gouvernance et de gestion établies en matière de sécurité de l'information à la Régie. Il peut définir, si nécessaire, des règles particulières en matière de gestion de l'information, incluant celles inhérentes à la sécurité de l'information, qui seront applicables à la Régie.

Le dirigeant réseau de l'information (DRI)

Désigné par le ministre de la Santé et des Services sociaux en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, le DRI veille à l'application, par les organismes publics qui lui sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information. Il peut définir, si nécessaire, des règles particulières en matière de gestion de l'information, incluant celles inhérentes à la sécurité de l'information, qui seront applicables à l'ensemble ou à une partie des organismes publics de son secteur.

Le responsable organisationnel de la sécurité de l'information (ROSI)

Désigné par le PDG en vertu de la Directive sur la sécurité de l'information gouvernementale, le ROSI représente le PDG en matière de sécurité de l'information auprès de la Régie et auprès du dirigeant principal de l'information.

Le coordonnateur organisationnel de gestion des incidents (COGI)

Désigné par le PDG en vertu de la Directive sur la sécurité de l'information gouvernementale, le COGI représente le PDG auprès du réseau d'alerte gouvernementale et y participe activement.

Le gestionnaire

Le gestionnaire s'assure que les activités relevant de son unité administrative sont réalisées dans le respect des principes directeurs énoncés dans la présente politique.

Le personnel de la Régie

Le personnel de la Régie est tenu de respecter les règles de sécurité applicables dans l'organisation.

DÉFINITIONS — Section facultative

Actif informationnel

Tout document ainsi que tout système d'information, appareil, réseau de télécommunication ou infrastructure technologique employé pour assurer sa conservation, son traitement, sa visualisation, sa transmission et son exploitation. En vertu de la Loi concernant le cadre juridique des technologies de l'information, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Cycle de vie de l'information

Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation.

Sécurité de l'information

Protection des ressources informationnelles d'une organisation, face à des risques identifiés, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée.

Régie de l'assurance maladie Québec

POLITIQUE
RI-1202

HISTORIQUE **Section obligatoire**

Description du changement	Instance	Date d'adoption
Adaptation au nouveau format des documents normatifs de la Régie	PDG	2016-05-05
Ajustement suite à l'entrée en vigueur de la Directive sur la sécurité de l'information gouvernementale en janvier 2014	PDG	2014-06-19
Mise à jour de l'annexe 1.	PDG	2009-12-11
Ajustement suite à l'entrée en vigueur de la Directive sur la sécurité de l'information gouvernementale en 2006.	PDG	2007-06-26
Nouveau document suite à la refonte complète du cadre normatif de la sécurité de l'information et à l'entrée en vigueur de la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale en 2000.	PDG	2003-03-18

Régie de l'assurance maladie Québec

POLITIQUE
RI-1202

ANNEXES **Section facultative**

Annexe 1

LOIS, RÈGLEMENTS ET DIRECTIVES APPLICABLES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Note : Cette information est présentée à titre indicatif seulement. Elle ne reflète pas nécessairement l'état actuel de l'ensemble des règles applicables.

LOIS

- Code Criminel (L.R.C. 1985, c. C-46)
- Charte des droits et libertés de la personne du Québec (RLRQ, chapitre A-2.1)
- Loi sur l'assurance maladie (RLRQ., chapitre A-29)
- Loi sur la Régie de l'assurance maladie du Québec (RLRQ, chapitre R-5)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03)
- Loi concernant le partage de certains renseignements de santé (RLRQ, chapitre P-9.0001)
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1)
- Loi sur la Fonction publique (RLRQ, chapitre F-3.1.1)
- Loi sur l'administration publique (RLRQ, chapitre A-6.01)
- Loi sur les archives (RLRQ, chapitre A-21.1)
- Loi sur le droit d'auteur (L.R.C., c. C-42)
- Loi sur les contrats des organismes publics (RLRQ, chapitre C-65.1)

RÈGLEMENTS

- Règlement sur l'éthique et la discipline dans la fonction publique (Loi sur la fonction publique)
- Règlement intérieur de la Régie de l'assurance maladie du Québec (Loi sur la Régie de l'assurance maladie du Québec)
- Règlement sur les formules et les relevés d'honoraires relatifs à la Loi sur l'assurance maladie (Loi sur la Régie de l'assurance maladie du Québec)
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels)
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (Loi sur les archives)
- Règles particulières du dirigeant réseau de l'information du secteur de la santé et des services sociaux (Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement)

DIRECTIVES

- Directive sur la sécurité de l'information gouvernementale (Loi sur l'administration publique)
- Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (Loi sur l'administration publique)
- Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire (Loi sur l'administration publique)
- Directive sur le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible (Loi sur l'administration financière)

Annexe 2

STRUCTURE DU CADRE NORMATIF
EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION