Commissaire à l'information et à la protection de la vie privée de l'Ontario

Feuille-info

Numéro 16
Juillet 2010

Le chiffrement fort dans les soins de santé

Le Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP), dans son ordonnance HO-004 et, plus récemment, dans son ordonnance HO-007, a exigé que les renseignements personnels sur la santé soient protégés en tout temps, plus précisément en veillant au chiffrement fort de ceux qui sont sauvegardés dans des appareils mobiles (p. ex., ordinateurs portables, cartes à mémoire flash, assistants numériques personnels)[1]. Cette ordonnance ne définit cependant pas ce qui constitue un « chiffrement fort » pour ce qui est de protéger la confidentialité, l'intégrité et l'accessibilité des renseignements personnels sur la santé.

Le présent document propose donc une définition du concept de chiffrement fort, et décrit les exigences fonctionnelles et techniques minimales de ce que doit représenter le chiffrement fort dans le contexte des soins de santé. Ces renseignements permettront d'établir des critères d'approvisionnement qui, s'ils sont respectés, feront en sorte que les renseignements personnels sur la santé sauvegardés dans des appareils ou des supports de données mobiles chiffrés demeurent accessibles aux utilisateurs autorisés mais à personne d'autre.

Nous tenons à remercier le Dr Robert Kyle, commissaire et médecin hygiéniste de la région de Durham, d'avoir appuyé la rédaction du présent document.

Le chiffrement fort

Introduction

Le terme « chiffrement fort » ne désigne pas une caractéristique technique ou une norme de conception précise, ni même une caractéristique de chiffrement particulière qui pourrait être incluse dans une spécification d'approvisionnement ou d'audit. Aucune technologie de chiffrement, aussi « forte » soit-elle, ne peut sécuriser les renseignements à elle seule. La protection des renseignements personnels contre l'accès non autorisé repose plutôt sur une variété de circonstances et de facteurs dont il faut tenir compte.

Pour commencer, il faut se servir d'un bon algorithme de chiffrement qui a été assujetti à un examen approfondi par les pairs. Ensuite, cet algorithme doit être implanté correctement; le seul moyen de le confirmer consiste à faire vérifier le système de chiffrement par un laboratoire indépendant de tests de sécurité. Une fois le système de chiffrement implanté, les clés de chiffrement doivent être protégées et gérées efficacement. Les utilisateurs qui sont autorisés à déchiffrer les données doivent être authentifiés de façon sécurisée au moyen de mots de passe, d'identificateurs biométriques ou de jetons de sécurité. Les systèmes ne doivent pas laisser des copies non chiffrées des données dans la mémoire cache des navigateurs Web ou sur des disques durs d'ordinateurs

portables, où un tiers non autorisé pourrait y avoir accès. Les utilisateurs autorisés doivent être enregistrés, recevoir une formation et être dotés d'un matériel adéquat. Les protections que confère le système de chiffrement doivent être activées par défaut, sans que les utilisateurs du domaine de la santé, qui sont déjà très occupés, n'aient à prendre de mesures particulières pour que les données demeurent chiffrées. Enfin, les renseignements personnels sur la santé doivent demeurer accessibles tout au long de leur cycle de vie, même si des mots de passe sont oubliés ou si des jetons de sécurité sont perdus.

À cause de ces exigences, les systèmes de chiffrement employés pour protéger la confidentialité des renseignements personnels sur la santé doivent posséder plusieurs caractéristiques.

Exigences techniques et fonctionnelles

Voici une description détaillée des exigences techniques concernant le chiffrement fort.

1. **Implantation sécurisée** : Le système de chiffrement doit répondre à une norme minimale pour la protection de renseignements délicats. Cette exigence comporte deux volets : premièrement, le système de chiffrement doit être conçu pour répondre à une norme minimale, et deuxièmement, les produits de chiffrement doivent être validés de façon indépendante en regard de normes pour confirmer qu'ils sont bien conçus et implantés correctement. Comme nous l'expliquons plus loin, la norme la plus appropriée et la plus courante s'appliquant aux systèmes de chiffrement pour les appareils mobiles est la FIPS 140-2[2], qui ne retient que quelques algorithmes. Le chiffrement fort exige l'utilisation d'appareils ou de logiciels certifiés conformes à la FIPS 140-2.

2. **Clés de chiffrement sécurisées et gérées** : Les clés de chiffrement doivent :

   2.1 être assez longues (d'une « taille » suffisante, mesurée en bits) pour résister à toute tentative visant à casser le chiffrement;

   2.2 demeurer protégées pour éviter leur vol ou leur divulgation à des personnes non autorisées.

3. **Authentification sécurisée des utilisateurs** : Avant le déchiffrement, les utilisateurs autorisés doivent être authentifiés de façon sécurisée (p. ex., au moyen d'un mot de passe fort) afin qu'eux seuls puissent déchiffrer les données et y accéder.

4. **Pas de création accidentelle de données non chiffrées** : Aucun fichier contenant des données déchiffrées ne devrait persister après qu'un utilisateur a accédé à des données chiffrées et les a visualisées ou mises à jour sous forme déchiffrée. Une copie des données déchiffrées ne doit pas exister à moins qu'un utilisateur autorisé n'en ait créé une délibérément.

Voici les exigences fonctionnelles que doivent respecter les systèmes de chiffrement afin de protéger la vie privée des clients tout en aidant les travailleurs de la santé à fournir des soins de qualité :

5. **Utilisateurs identifiés, autorisés et bien formés** : Les dépositaires de renseignements sur la santé devraient pouvoir déterminer en tout temps les utilisateurs qui ont accès à des renseignements chiffrés au moyen d'un appareil mobile ou d'un support mobile de

données précis. C'est dire que les utilisateurs qui sont autorisés à accéder à des données chiffrées ou à les mettre à jour doivent être identifiés individuellement au préalable et recevoir des jetons d'authentification (p. ex., un mot de passe fort) approprié. Les utilisateurs doivent aussi recevoir une formation adéquate sur la façon d'accéder aux renseignements chiffrés et d'en assurer la protection.

6. **Chiffrement par défaut** : Lorsqu'un système de chiffrement a été installé sur un appareil ou un support de données mobile, le chiffrement devrait avoir lieu sans que les utilisateurs n'aient à l'activer pour protéger les données.

7. **Accessibilité et protection de l'information pendant son cycle de vie** : Il faut avoir l'assurance raisonnable que les données chiffrées demeureront accessibles (p. ex., même si l'on oublie les mots de passe, si le personnel n'est pas disponible pour cause de maladie ou de décès, etc.). Pour ce faire, il faut assurer une gestion centralisée des mots de passe et autres jetons d'authentification. Il faut aussi pouvoir faire des copies de sécurité des fichiers ou supports chiffrés, comme dans le cas des autres fichiers (déchiffrés).

Tous ces facteurs s'appliquent lorsque le chiffrement est employé pour sécuriser les données sauvegardées dans des appareils et supports mobiles comme des ordinateurs portables, des téléphones cellulaires, des disques durs portatifs et des cartes mémoire flash. Ils s'appliquent également au chiffrement employé pour sécuriser des communications, par exemple, les réseaux privés virtuels, les systèmes de courrier électronique protégés et l'accès Web protégé. Cependant, il faut aussi tenir compte d'un dernier facteur fonctionnel lors de la conception et de l'implantation d'infrastructures de technologie de l'information (TI) :

8. **Évaluation des menaces et des risques** : Les infrastructures de TI qui recourent à des technologies de sécurité comme le chiffrement devraient être soumises à une évaluation des menaces et des risques avant leur mise en service (et de préférence avant leur implantation) pour s'assurer qu'elles fonctionnent correctement.

Chacune des exigences précédentes est décrite en détail ci-dessous.

1. Implantation sécurisée

La technologie du chiffrement a évolué rapidement au cours des dix dernières années, et des algorithmes de chiffrement qui étaient autrefois acceptables, comme la norme de chiffrement de données (Data Encryption Standard, DES) et la confidentialité équivalente aux transmissions par fil (Wired Equivalent Privacy, WEP), sont maintenant considérées comme étant beaucoup trop faibles pour que l'on puisse s'y fier. En outre, des fournisseurs ont créé de nombreux algorithmes exclusifs dont on a découvert par la suite qu'ils présentaient des failles. Heureusement, il existe des normes de chiffrement reconnues; ces normes précisent clairement les algorithmes acceptables, que les fournisseurs ont intégrés correctement dans leurs produits.

La norme la plus répandue pour les modules cryptographiques est la Federal Information Processing Standard (FIPS) 140-2, publiée par le National Institute for Standards in Technology (NIST) des États-Unis. Le Programme de validation des modules cryptographiques

(PVMC) valide des modules cryptographiques selon la FIPS 140-2 et d'autres normes de cryptographie. Le PVMC a été instauré conjointement par le NIST et le Centre de la sécurité des télécommunications Canada (CSTC) du gouvernement du Canada. Les produits jugés conformes à la FIPS 140-2 sont reconnus par les organismes fédéraux des deux pays pour la protection de renseignements délicats (États-Unis) ou de renseignements désignés (Canada). Les fournisseurs de modules cryptographiques font appel à des laboratoires d'essai indépendants et accrédités pour faire tester leurs modules. Le CSTC accrédite ces laboratoires au Canada.

En plus de l'accréditation, la FIPS 140-2 décrit un élément essentiel de tout système de chiffrement : des algorithmes de chiffrement adéquats. L'annexe A de la FIPS 140-2 énumère les trois algorithmes de chiffrement qui sont approuvés. Deux d'entre eux sont d'usage courant pour le chiffrement des appareils mobiles : l'Advanced Encryption Standard (AES) et le Triple DES[3]. L'un ou l'autre peut être employé dans les systèmes de chiffrement validés selon la FIPS 140-2.

2. Clés de chiffrement sécurisées

L'AES s'utilise avec des clés de 128, 192 et 256 bits, qui sont toutes considérées comme sécuritaires pour l'usage courant. Toutefois, pour cet algorithme, les clés de 128 bits pourraient être trop courtes pour la sauvegarde à long terme de renseignements délicats, surtout si les données chiffrées doivent être archivées pendant de nombreuses années. L'algorithme Triple DES s'utilise avec des clés de 112 et 168 bits; celles de 112 bits ne sont plus couramment utilisées pour la sauvegarde de renseignements délicats.

Il est préférable de conserver les clés de chiffrement sur un support doté de caractéristiques cryptographiques comme une clé USB, une carte à puce ou un ordinateur portable équipé d'un module cryptographique. En l'absence de protection matérielle, les clés doivent être protégées par des modules logiciels qui les chiffrent et qui donne accès uniquement à un programme cryptographique autorisé. Ce programme, à son tour, peut être activé uniquement par des utilisateurs dûment authentifiés.

3. Authentification sécurisée des utilisateurs

Les systèmes de chiffrement en vente dans le commerce proposent une foule de moyens d'utiliser des supports et appareils mobiles, notamment l'utilisation de mots de passe forts (composés à la fois de caractères alphabétiques, de caractères spéciaux et de chiffres, au nombre d'au moins huit), des lecteurs biométriques d'empreintes digitales (pour les appareils mobiles et les clés USB) et des porte-clés USB (dans le cas des appareils mobiles comme les ordinateurs portables). La méthode d'authentification choisie, quelle qu'elle soit, doit être en mesure d'interdire l'accès aux utilisateurs non autorisés qui tentent de se faire passer pour des utilisateurs autorisés.

4. Pas de création accidentelle de données non chiffrées

Il ne doit pas exister de copie des données déchiffrées à moins qu'un utilisateur autorisé n'en ait créé une délibérément. Les systèmes de chiffrement mal conçus peuvent laisser des copies de données chiffrées sous une forme déchiffrée dans un fichier temporaire

sauvegardé sur le disque dur d'appareils mobiles, comme un ordinateur portable. Cela peut se produire, par exemple, si le fournisseur du produit de chiffrement a négligé de tenir compte de situations telles qu'une panne de courant qui surviendrait pendant l'utilisation de l'ordinateur. Certains systèmes Web sont également mal conçus du fait qu'ils permettent aux navigateurs de conserver dans leur mémoire cache des copies déchiffrées de données qui ont été acheminées à l'utilisateur de façon sécurisée par le protocole SSL (Secure Sockets Layer). Voir plus loin l'exposé sur l'évaluation des menaces et des risques.

5. Utilisateurs identifiés, autorisés et bien formés

Dans le domaine des soins de santé, il est insuffisant, en règle générale, de se contenter d'authentifier les utilisateurs en leur donnant tous le même mot de passe, par exemple. Dans ce cas, après le départ d'un seul membre du personnel, il faudrait donner un nouveau mot de passe à des dizaines, voire des centaines d'autres utilisateurs. En outre, le partage de mots de passe ne permettrait généralement pas aux dépositaires de renseignements sur la santé de confirmer avec précision qui a accédé à un dossier ou à une base de données en particulier. Les utilisateurs qui sont autorisés à accéder à des données chiffrées ou à les mettre à jour doivent être identifiés individuellement au préalable et recevoir un nom d'utilisateur unique ainsi que des jetons d'authentification (p. ex., mots de passe forts) appropriés. Quel que soit le système de contrôle d'accès employé pour faire le suivi des utilisateurs et leur attribuer un nom d'utilisateur, ce système doit s'harmoniser avec le système de chiffrement choisi.

Enfin, il faut faire confiance uniquement aux utilisateurs qui ont reçu une formation appropriée pour l'accès aux données chiffrées et la protection de leur confidentialité tout au long de leur utilisation.

6. Chiffrement par défaut

Les fournisseurs de soins de santé n'ont pas le temps de vérifier un fichier de données chiffrées chaque fois qu'ils le consultent ou le mettent à jour pour s'assurer que le système de chiffrement fonctionne encore et que les données demeurent chiffrées. Une fois installé, le système de chiffrement doit continuer de protéger les données chiffrées de façon fiable sans qu'il ne soit nécessaire pour les utilisateurs de le régler et de le mettre à l'essai régulièrement.

7. Accessibilité et protection de l'information pendant son cycle de vie

Les renseignements personnels sur la santé utilisés pour la fourniture de soins de santé doivent être accessibles en tout temps; c'est pourquoi les systèmes de chiffrement doivent permettre d'y accéder chaque fois qu'on en a besoin. Si le système rend les données illisibles en permanence lorsqu'un utilisateur n'est plus disponible (p. ex., en cas de décès, de maladie ou d'un autre événement semblable), ou simplement lorsqu'un utilisateur oublie son mot de passe, il n'est pas approprié pour les soins de santé. Heureusement, différents fournisseurs proposent une variété de produits qui comportent des fonctions de gestion centralisée permettant l'établissement de mots de passe illimités, l'attribution de nouveaux mots de passe à distance et d'autres moyens de faciliter la mise en service et la gestion

d'un grand nombre d'appareils ou de supports mobiles sans que l'on craigne de perdre des données.

Par ailleurs, les systèmes de chiffrement doivent permettre de faire, selon un horaire établi, une copie de sécurité des fichiers de données chiffrées, ou à tout le moins ne pas nuire au fonctionnement des systèmes de copie de sécurité déjà installés.

8. Évaluation des menaces et des risques

Le chiffrement doit être adapté et proportionnel aux menaces et risques connus : perte ou vol d'un appareil portable, négligence ou formation insuffisante du personnel, malveillance, piratage, etc. À moins de définir et d'évaluer les menaces et les risques pour leurs données de façon méthodique, objective et crédible, les organismes qui mettent sur pied de grandes infrastructures de TI ne pourront déterminer s'ils ont implanté correctement leur système de chiffrement. Le meilleur moyen de le savoir consiste à mener une évaluation des menaces et des risques (EMR). Heureusement, il existe une méthodologie d'EMR qui est courante et reconnue; elle a été établie conjointement par le Centre de la sécurité des télécommunications Canada et la GRC, et est accessible à www.cse-cst.gc.ca/its-sti/publications/tra-emr/index-fra.html.

En Ontario, les fournisseurs de réseaux d'information sur la santé sont tenus d'effectuer une évaluation des menaces et des risques conformément à la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*) et à ses règlements d'application[4].

Autres documents pertinents du CIPVP

Ordonnance HO-008 rendue en vertu de la *LPRPS* (juin 2010)

Ordonnance HO-007 rendue en vertu de la *LPRPS* : *Encrypt Your Mobile Devices: Do It Now* (janvier 2010)

Ordonnance HO-004 rendue en vertu de la *LPRPS* (mars 2007)

Feuille-info n° 12 : *Le chiffrement des renseignements personnels sur la santé dans les appareils mobiles* (mai 2007)

Feuille-info n° 13 : *Technologies de communication sans fil : les systèmes de surveillance vidéo* (juin 2007)

Feuille-info n° 14 : *Technologies de communication sans fil : protection de la vie privée et sécurité* (août 2007)

Lectures suggérées

Normes FIPS : http://csrc.nist.gov/publications/PubsFIPS.html

Liste de produits de chiffrement certifiés selon la FIPS 140 : http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

ISO/IEC 19790:2006 – *Security requirements for cryptographic modules*

ISO 27799 : *Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002*

Le document d'orientation suivant du gouvernement de l'Ontario est destiné aux ministères, mais il contient des renseignements utiles sur la gestion du chiffrement et des mots de passe. Voir notamment l'annexe A, Approved Algorithms and Protocols.

Government of Ontario IT Standard (GO-ITS) 25.12: Security Requirements for the Use of Cryptography Version #: 1.1 (2008), à www.mgs.gov.on.ca/en/IAndIT/258071.html.

NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Au sujet de Ross Fraser

Ross Fraser est un expert reconnu de la protection de la vie privée et de la sécurité dans le domaine des soins de santé. Il fait des exposés sur la confidentialité, l'authentification, la cryptographie et les signatures numériques au Canada, aux États-Unis et au Royaume-Uni, et il a rédigé des politiques de sécurité et implanté des systèmes de sécurité pour des sociétés privées, des gouvernements et ministères de la Santé au Canada et le National Health Service de Grande-Bretagne ainsi que des organismes de santé à but non lucratif. M. Fraser a également siégé pendant six ans comme responsable du groupe de travail sur la sécurité de l'informatique de santé de l'Organisation mondiale de normalisation (ISO) et a été rédacteur principal de quatre normes internationales sur la sécurité dans les soins de santé.

---

1. Voir www.ipc.on.ca/images/Findings/ho-007.pdf.
2. Voir http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
3. L'algorithme Triple DES est défini dans ISO/IEC 18033-3:2005 Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers.
4. La disposition 5 du par. 6 (3) du Règl. de l'Ont. 329/04 pris en application de la *LPRPS* est libellée comme suit : « Le fournisseur [d'un réseau d'information sur la santé] évalue les services qui ont été fournis aux dépositaires de renseignements sur la santé concernés à l'égard des points suivants et remet à chacun d'eux une copie des résultats obtenus : i) les menaces, la vulnérabilité et les risques qui existent en matière de protection et d'intégrité des renseignements personnels sur la santé […] ».Voir http://www.lois-en-ligne.gouv.on.ca/html/regs/french/elaws_regs_040329_f.htm.

Feuille-info

est publié par **le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.**

Pour nous faire part de vos observations, nous informer d'un changement d'adresse ou pour que votre nom soit ajouté à la liste d'envoi, veuillez communiquer avec :

Service des communications
Commissaire à l'information et
à la protection de la vie privée de l'Ontario
2 rue Bloor Est, Bureau 1400
Toronto (Ontario) CANADA
M4W 1A8
Téléphone : 416-326-3333 • 1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca
This publication is also available in English.

papier recyclé à 30%

ISSN 1188-3006