Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la Santé et des Services sociaux
AVRIL 1992

TABLE DES MATIÈRES
LES ORIENTATIONS DE LA COMMISSION

LES ORIENTATIONS DE LA COMMISSION

INTRODUCTION

Ce document s'inscrit dans la nouvelle approche de la Commission d'accès à l'information, appelée « Approche par problématique ».

Depuis l'implantation de cette approche, la Commission étudie et se prononce sur l'ensemble des phénomènes en rapport avec la protection des renseignements personnels et l'accès à l'information. Elle émet des orientations, des recommandations ou des lignes directrices sur la problématique choisie. Cette approche est préventive et s'adresse à tous les organismes concernés par la problématique privilégiée.

La problématique visée par le présent document est l'informatisation des dossiers des bénéficiaires du réseau de la Santé et des Services sociaux. Au cours de l'automne 1991, ce document a fait l'objet de consultations étendues et peut ainsi proposer des mesures réalistes, applicables par les organismes du réseau.

La Commission désire rappeler aux organismes les droits fondamentaux des personnes en perte d'autonomie physique, psychologique et sociale, et plus spécifiquement leur droit au respect de la vie privée. Ce droit s'applique à tous les citoyens mais il devient d'autant plus important à protéger lorsque la personne, en situation de dépendance, doit communiquer des renseignements personnels.

La Commission incite donc les organismes du réseau de la Santé et des Services sociaux à faire preuve de vigilance et de prudence lors de l'élaboration et de l'implantation des systèmes informatiques. Ce guide leur permettra d'être conformes à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et d'éviter d'éventuelles poursuites en vertu de la *Charte des droits et libertés de la personn*e, de la *Loi sur les services de santé et les services sociaux* et de la *Loi sur l'acc*ès. Mais ils pourront aussi obtenir aide et assistance du personnel de la Commission.

PROBLÉMATIQUE

Depuis quelques années, l'informatique ne cesse de s'imposer dans les dossiers des bénéficiaires du réseau de la Santé et des Services sociaux. Ce sont les projets les plus importants et impliquant plusieurs centres hospitaliers qui ont d'abord attiré l'attention du public et de la Commission d'accès à l'information.

Actuellement, en 1992, l'informatisation des dossiers est très inégale. Dans certains centres hospitaliers, elle est relativement avancée et utilisée quotidiennement par la majorité des départements tandis que dans les centres d'accueil, par exemple, elle est encore embryonnaire. La Commission ne se prononcera pas sur les avantages et les inconvénients de l'informatisation des dossiers des usagers car le phénomène est irréversible et sera bientôt la norme dans tout le réseau de la Santé et des Services sociaux.

Conformément aux pouvoirs qui lui sont conférés par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnel*s, la Commission désire toutefois s'assurer que la confidentialité des dossiers des bénéficiaires continuera d'être garantie. Tous les experts conviennent que les risques de rupture de la confidentialité des dossiers informatiques sont suffisamment importants pour que la sécurité de ces dossiers constitue une préoccupation majeure. Les possibilités de traitement, de croisement, d'appariement de données sont quasiment illimitées; là se trouve la grande menace à la confidentialité. Très rapidement, comme jamais auparavant, des centaines, voire des milliers de données peuvent faire l'objet de traitements grâce à des systèmes informatiques de plus en plus conviviaux, c'est-à-dire de plus en plus accessibles à des profanes. De plus, les interconnexions de systèmes sont relativement faciles et peuvent susciter des "besoins" d'utilisation d'informations personnelles à d'autres fins que celles initialement prévues lors de leur cueillette.

OBJECTIF DU DOCUMENT

Rappelons, d'abord, l'expérience de la Commission concernant les dossiers des usagers détenus sur support papier. Les risques de manquement à la confidentialité sont là aussi réels et il ne faut pas les minimiser; dans plusieurs cas la Commission a dû enquêter, et a pu constater que des personnes non autorisées avaient eu accès à des dossiers de bénéficiaires. La vigilance des organismes doit donc être constante pour assurer le caractère confidentiel des dossiers détenus, quel qu'en soit le support.

En publiant ce document, la Commission poursuit un objectif pédagogique, de conseil et d'assistance auprès des organismes du réseau de la Santé et des Services sociaux. La Commission veut s'assurer que l'informatisation respectera les principes reconnus dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Elle souhaite aider autant les responsables des organismes que les gestionnaires et les concepteurs qui désirent implanter des systèmes informatiques.

Ce document énumère et décrit les mesures de sécurité que la Commission considère comme minimales afin de garantir la confidentialité des dossiers informatisés.

Ces mesures sont basées sur la *Charte des droits et libertés de la personne*, qui consacre le droit au respect de la vie privée, et sur les principes de la *Loi sur l'accès*.

LES GRANDS PRINCIPES DE LA *LOI SUR L'ACCÈS*

Ces principes s'articulent autour de la collecte, de la confidentialité et de l'accès aux renseignements personnels.

1. La collecte de renseignements nominatifs

La Loi sur l'accès prescrit, à l'article 64, les règles relatives à la cueillette de renseignements personnels :

> 64. Nul ne peut, au nom d'un organisme public, recueillir un renseignement nominatif si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a gestion.

Le ministère de la Santé et des Services sociaux, la Régie de l'assurance-maladie, les régies régionales et les établissements du réseau de la santé et des services sociaux doivent donc s'interroger sur la nécessité de chaque information nominative avant de la recueillir auprès de la personne concernée. L'implantation du système informatisé des dossiers des usagers en fournit l'occasion aux dirigeants des organismes; certaines informations pourront ne plus être colligées si elles ne sont pas indispensables à l'organisme pour dispenser ses services. Par exemple, quelques hôpitaux demandent à leurs patients, lors de leur inscription, quelle est leur religion. Ce renseignement est-il nécessaire ou tout simplement souhaitable? S'il est nécessaire, l'hôpital pourra évidemment le colliger. Il est à souligner que la Commission a déjà interprété la notion de « renseignement nécessaire » et lui a donné le sens d'« indispensable ».

2. La confidentialité des renseignements nominatifs et leur communication

Le dossier des usagers est soumis à la plus stricte confidentialité. L'article 53 de la *Loi sur l'accès* et l'article 19 de la *Loi sur les services de santé et les services sociaux* stipulent qu'aucun renseignement ne peut être tiré du dossier sans le consentement de l'individu concerné.

La Commission privilégie pour sa part un consentement libre, éclairé et donné par écrit par la personne concernée. Nous rappelons par ailleurs que souvent, les informations demandées ne concernent pas toujours l'ensemble du dossier de la personne. La Commission de la santé et de la sécurité du travail du Québec, par exemple, ne requiert, par consentement écrit, que les renseignements relatifs à la lésion professionnelle. Le centre hospitalier ne doit donc pas transférer tout le dossier médical de ce travailleur.

Ce même article 19 de la *Loi sur les services de santé et les services sociaux* prévoit des exceptions au principe du consentement. Dans ces cas bien particuliers -et exceptionnels-, les informations peuvent être transférées en autant que leur confidentialité soit garantie.

3. L'accès aux données nominatives

En vertu de l'article 83 de la *Loi sur l'accès* et de l'article 17 de la *Loi sur les services de santé et les services sociaux*, l'usager a le droit de consulter son dossier ou d'en obtenir copie. Les systèmes informatiques doivent prévoir cette possibilité; les droits d'accès des patients demeurent les mêmes que lorsque le dossier est détenu sur

support papier. Les centres hospitaliers doivent prendre ces droits en considération si des terminaux sont installés dans la chambre des bénéficiaires.

L'accès aux données nominatives des bénéficiaires par le personnel des organismes de la Santé et des Services sociaux pose cependant problème. Chaque système doit prévoir des droits d'accès différents selon les catégories d'employés : ainsi les employés du Service des finances d'un organisme ne doivent évidemment pas avoir les mêmes droits d'accès que le personnel clinique. Cet exemple est extrême, mais il illustre bien la nécessité de la segmentation des accès selon la fonction des employés. De même, les possibilités de consultation, d'inscription, de modification et de destruction des renseignements sociosanitaires devront aussi être différentes selon qu'il s'agit du personnel au Service d'admission, au Service diététique, au Service de santé et sécurité du travail ou au Service d'adoption.

LES MESURES DE SÉCURITÉ MINIMALES.

OBJET

Cette partie précise les mesures de sécurité qu'un organisme du secteur de la Santé et des Services sociaux doit mettre en application pour assurer le caractère confidentiel et l'intégrité des données sociosanitaires nominatives informatisées qu'il détient.

ORGANISMES ASSUJETTIS

Les organismes soumis à l'application des mesures présentées dans ce document sont les organismes de la Santé ou des Services sociaux, assujettis à la *Loi sur l'accès* : le ministère de la Santé et des Services sociaux, la Régie de l'assurance-maladie, les régies régionales et tous les établissements du réseau.

DOMAINE D'APPLICATION

Les données sociosanitaires nominatives visées par les mesures présentées dans ce document sont toutes celles qu'un organisme de la Santé ou des Services sociaux emmagasine dans son ordinateur central, dans celui de son fournisseur de services informatiques ou sur micro-ordinateur. En fait tout matériel informatique qui conserve, transmet, traite est concerné, de même que tout support : bandes magnétiques, disquettes, listes ou microfilms de sorties d'ordinateur, etc.

DONNÉES NOMINATIVES

Les mesures de sécurité décrites dans ce document concernent les renseignements nominatifs dans le secteur de la Santé et des Services sociaux. Qu'est-ce qu'un renseignement nominatif? Les articles 54 et 56 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* en fournissent les caractéristiques:

> 54. Dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier.
>
> 56. Le nom d'une personne physique n'est pas un renseignement nominatif, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement nominatif concernant cette personne.

À la lecture de ces articles, on constate que dans le domaine d'application de la présente politique, presque toutes les informations détenues sont nominatives. Les organismes devront être très prudents lorsqu'ils auront à déterminer le caractère nominatif de chaque renseignement. En effet, un renseignement seul peut ne pas permettre d'identifier une personne en particulier; par contre si ce renseignement est joint à un autre, l'individu pourra plus facilement être identifié. Ainsi un numéro de dossier seul ne permet pas de repérer une personne, mais si on y ajoute le nom de l'établissement, les possibilités d'identification sont réelles. Ces deux renseignements combinés doivent donc être considérés comme nominatifs.

Peu importe le support sur lequel les données sociosanitaires sont conservées par un organisme, elles.peuvent faire l'objet de divulgations ou d'altérations, accidentelles ou volontaires, dans des circonstances aussi diverses que celles-ci : les inondations, les tremblements de terre, les incendies, le vandalisme, le sabotage, les pannes affectant le matériel, les erreurs de saisie, de transmission ou d'exploitation, la fraude, la falsification, la modification, l'ajout, la destruction, le vol de matériel ou de données sociosanitaires...

Nous présentons ici des mesures de sécurité ou des dispositifs minimaux qui permettront de respecter les grands principes de la *Loi sur l'accès* et de contrer ces événements (certains organismes, pour assurer une meilleure protection de leurs données sociosanitaires, pourraient être obligés d'en implanter d'autres encore plus sécuritaires). À l'instar de la plupart des organismes consultés, la Commission est convaincue que ces mesures de sécurité seront efficaces si le personnel y est sensibilisé régulièrement. Les mesures de sécurité les plus sophistiquées seront performantes seulement si ceux et celles qui les appliquent sont persuadés de leur bien-fondé.

Par conséquent, si un organisme veut déterminer les mesures de sécurité les mieux appropriées à son cas, il devra faire une évaluation des possibilités de risques dans son milieu. Cette évaluation est communément appelée : **analyse de risques**.

ACTIONS QUE LES ORGANISMES DOIVENT POSER

Pour implanter et faire respecter les mesures de sécurité, les organismes doivent élaborer et maintenir à jour des politiques et procédures. Pour arriver à ces fins, les organismes doivent nommer une personne responsable qui aura l'appui non équivoque de la haute direction.

Pour la Commission, une personne est déjà toute désignée : il s'agit du responsable de la protection des données personnelles dont le rôle, déjà déterminé par la *Loi sur l'accè*s, est de s'assurer du caractère confidentiel des données sociosanitaires.

Pour l'aider à réaliser son mandat et lorsque les fonctions de l'organisme le justifient, cette personne devrait créer et présider un comité sur la sécurité des données sociosanitaires. Ce comité aurait les responsabilités suivantes:

- développer un programme de sensibilisation et de formation du personnel en matière de sécuritéet de protection des données sociosanitaires;
- coordonner toutes les activités reliées à la protection des données sociosanitaires et à la sécurité informatique (mise en place de mécanismes appropriés, tels le maintien de profils d'accès, la
- vérification des accès, la gestion des codes d'identification et des cartes à barres, etc.);
- vérifier périodiquement que le programme de sécurité et de protection des données sociosanitaires est respecté (cette tâche devrait être effectuée par le vérificateur interne ou externe ou du moins par une personne indépendante des différents groupes de sécurité);
- produire un bilan annuel (suivi et contrôle) de l'application du programme de sécurité à la personne ayant la plus haute autorité au sein de l'organisme.

La situation étant différente d'un organisme à l'autre, l'intention de la Commission n'est pas d'indiquer qui devrait faire partie de ce comité. Ce choix incombera aux gestionnaires des établissements.

MESURES DE SÉCURITÉ

En vue de protéger les données sociosanitaires informatisées contre toute divulgation ou altération, les mesures ou dispositifs de sécurité doivent au moins couvrir les aspects suivants : l'identification et l'authentification des utilisateurs au regard de l'accès aux données sociosanitaires, les profils d'accès, la collecte ou la saisie des données, les copies de sécurité, les terminaux, l'ordinateur central, la journalisation des accès, les télécommunications, tout mandat confié par un organisme à une personne ou à un autre organisme (pour l'informatique ou les services de bureau, par exemple), le partage de bases de données communes ou d'un centre de traitement commun, un programme de sensibilisation et d'embauche de personnes, la communication de données sociosanitaires, les micro-ordinateurs, l'impression des données sociosanitaires.

1. Identification et authentification des utilisateurs au regard de l'accès aux données sociosanitaires

- Pour pouvoir accéder aux données sociosanitaires informatisées auxquelles ils ont droit, les utilisateurs doivent d'abord s'identifier. Il existe différents mécanismes d'identification :
  l'utilisateur peut inscrire son code d'identification à l'aide du clavier, au moyen d'une carte à barres, d'une carte à microprocesseur, d'une clé magnétique, par exemple.
- Un code d'identification ne doit être assigné qu'à un seul utilisateur. Si l'utilisateur doit avoir accès à plus d'un poste de travail en même temps, il a droit à plusieurs codes d'identification.
  Deux utilisateurs ne doivent cependant jamais partager le même code d'identification.
- Tous les codes d'identification qui n'ont pas été utilisés pendant une période donnée doivent être désactivés ou détruits, à la suite d'une vérification préalable.
- Chaque établissement doit se doter de politiques et de procédures administratives pour l'attribution des codes d'identification.
- À un code d'identification doit être ajoutée l'authentification des utilisateurs. Cette authentification peut se faire par l'entrée d'un mot de passe, ou par des moyens biométriques :
  empreintes de la main, enregistrement de la voix, image de la rétine de l'oeil, etc.
- Les mots de passe peuvent être composés de caractères ou de chiffres et doivent comporter entre cinq et huit positions.
- Les mots de passe des utilisateurs ne doivent pas être affichés aux écrans.
- Les utilisateurs doivent changer leurs mots de passe périodiquement : au moins une fois tous les trois mois si le code d'identification est entré au moyen du clavier, au moins tous les six mois si le code d'identification est entré par un autre moyen (carte à barres, carte à microprocesseur, clé magnétique, etc.). Un organisme peut également déterminer la fréquence de changement du mot de passe en considérant le nombre d'accès au système par un utilisateur au cours d'une période donnée.
- Après un maximum de cinq erreurs d'inscription de son mot de passe, l'accès d'un utilisateur doit être refusé.
- Toute personne qui reçoit un code d'identification et un moyen d'authentification pour accéder aux données sociosanitaires doit s'engager à ne pas les divulguer ou les prêter et, le cas échéant, à en assumer la responsabilité.
- Le supérieur immédiat, ou une autre personne spécialement mandatée doit révoquer ou suspendre le code d'identification et le moyen d'authentification d'un utilisateur :
  - lorsque cet utilisateur quitte définitivement l'organisme ou est congédié;
  -.lorsqu'il a terminé son contrat;
  - lorsqu'il change de fonctions à l'intérieur de l'organisme et que ses nouvelles fonctions n'exigent pas l'accès aux données sociosanitaires;
  - lorsqu'il y a abus ou indice d'usage abusif;
  -.lorsque l'utilisateur doit s'absenter pour une période déterminée par l'organisme.

2. Les profils d'accès

- Les utilisateurs ne doivent avoir accès qu'aux dossiers sociosanitaires nécessaires à l'exercice de leurs fonctions. Les organismes doivent donc définir pour chacun des utilisateurs un "profil d'accès" qui déterminera ce à quoi il a accès (administration, médical, social) ainsi que le mode d'accès (écriture, lecture...). À cause des situations d'urgence, il faut prévoir tous les accès nécessaires possibles.
- Les établissements doivent avoir des profils d'accès différents pour leurs employés, selon que les dossiers des usagers sont actifs ou inactifs. Dans le cas des dossiers inactifs, il incombe à l'archiviste, ou à une personne désignée qui remplit ce rôle, d'avoir accès à ces dossiers, et de les rendre actifs au besoin.
- Le personnel de développement informatique ne doit pas avoir accès aux données sociosanitaires nominatives réelles et aux systèmes de production. En fait, le personnel de développement informatique ne doit avoir accès aux données sociosanitaires réelles que si elles sont dénominalisées. Quant au personnel de support informatique, il a accès aux systèmes de production si c'est nécessaire (en cas de panne, par exemple).
- Les organismes doivent utiliser des données sociosanitaires fictives ou dénominalisées lorsqu'ils donnent de la formation ou font des présentations. Les stagiaires qui travaillent auprès des bénéficiaires, bien qu'ils soient en formation, peuvent toutefois utiliser des données sociosanitaires réelles si cela s'avère nécessaire à leur formation.
- Les accès aux données sociosanitaires ou aux résultats de laboratoire sont permis à partir du domicile de l'usager lors de soins chez lui, ou à partir du domicile ou de la clinique d'un médecin ou d'un professionnel spécialisé en autant qu'il s'agisse d'un dossier ou de résultats de laboratoire concernant l'usager traité par ce médecin ou ce professionnel spécialisé.
- Sous réserve de la *Loi sur les archive*s, l'accès à la fonction de destruction des données sociosanitaires doit être limité à quelques intervenants et à des conditions très précises.
- La destruction des données sociosanitaires doit être faite de façon à ce que leur caractère confidentiel soit protégé.
- Chaque organisme doit se doter de politiques et procédures administratives pour l'attribution des profils d'accès à leur personnel.

3. Au regard de la collecte (saisie)

- Seules les personnes autorisées par l'organisme peuvent recueillir, inscrire ou faire inscrire des données cliniques au dossier informatisé d'un usager.
- Un organisme doit pouvoir identifier toute personne qui inscrit une donnée socio-sanitaire dans le dossier d'un bénéficiaire : les données cliniques inscrites seront donc authentifiées. Afin d'éviter que l'authenticité de ces éléments informatisés ne soit contestée, le logiciel utilisé sera conçu de façon à que les données déjà inscrites ne puissent être effacées. Comme il est cependant possible d'effectuer des additions correctrices à ces données, une mention indiquant l'auteur et le moment de la modification doit être présente.

- Un organisme ne doit recueillir que les données sociosanitaires pertinentes, exactes et nécessaires aux services à l'usager, à la santé publique ainsi qu'au suivi des opérations, à la gestion et à la planification des services.

4. Copies de sécurité

- Des copies de sécurité des données sociosanitaires, des programmes et des logiciels doivent être faites périodiquement.
- Seul un nombre restreint de personnes sera autorisé à faire ces copies.
- Chaque organisme doit déterminer quelles sont les personnes responsables qui effectueront les copies.
- Les copies de sécurité doivent être conservées dans un autre local que celui où est installé l'ordinateur et, si possible, dans un autre édifice.
- La circulation de ces copies doit être contrôlée.

5. Les terminaux

- Les terminaux doivent être installés dans des locaux (zones de travail) à accès restreint ou pouvant être verrouillés; s'ils ne peuvent être dans de tels locaux (c'est par exemple le cas des terminaux se trouvant au chevet d'un patient), il faut alors doter les terminaux d'une serrure ou d'un lecteur de carte magnétique.
- Lorsque des données nominatives apparaissent à l'écran, les organismes doivent annuler toute session de travail d'un utilisateur qui, après une période donnée, n'a effectué aucune transaction à son terminal (cette période, qui devrait être la plus courte possible, sera déterminée par l'établissement et variera d'un terminal à l'autre, selon les fonctions de l'utilisateur).
- Lorsque des données nominatives apparaissent à l'écran, il faut faire en sorte que les personnes non autorisées ne puissent pas visualiser ce qui apparaît à l'écran (une bonne disposition des écrans ou des isoloirs appropriés y contribueront).

6. Sécurité des lieux

Les organismes doivent protéger adéquatement les locaux où sont installés leurs ordinateurs et les lignes de communication, et en restreindre l'accès aux seules personnes autorisées.

7. Journalisation des accès

Tous les accès aux renseignements nominatifs doivent être journalisés. La journalisation permettra obligatoirement de connaître :

1- le code d'identification de l'utilisateur;
2- le nom du fichier auquel il a eu accès;
3- le numéro du dossier concerné;
4- l'accès en cause (création, lecture, modification, destruction d'un dossier);
5- le code de transaction ou le nom du programme (indiquer le plus précis des deux);
6- la date (année, mois, jour) de l'accès; 7- l'heure (heure, minute, seconde) de l'accès.

Ces informations peuvent être emmagasinées dans les dossiers des usagers ou dans un fichier séparé.

- Les accès non autorisés doivent être vérifiés.
- Pour les tâches d'impression des données nominatives de tous les dossiers d'un fichier, il n'est pas nécessaire de journaliser les numéros de dossiers concernés; les autres items mentionnés précédemment doivent cependant l'être.
- Pour les tâches d'impression des données dénominalisées ou statistiques, il n'est pas nécessaire d'effectuer une journalisation.
- Ces journalisations doivent être conservées pendant deux ans; cependant, si une enquête ou des procédures judiciaires sont instituées, elles devront être conservées tant que l'affaire ne sera pas réglée.
- Avec la journalisation des accès, l'informatisation des dossiers des bénéficiaires permet de repérer aisément l'employé qui aurait pris connaissance sans raison du dossier d'un bénéficiaire. Des sanctions peuvent donc être prises à l'endroit de ces personnes.

8. Télécommunications

- Afin de détecter la présence d'anomalies ou une utilisation frauduleuse des télécommunications, des contrôles doivent être effectués périodiquement sur les mots de passe et les privilèges d'accès attribués aux usagers.

- Les télécommunications seront effectuées dans un cadre assurant que les données nominatives communiquées ne peuvent pas être interceptées ou introduites par un terminal non autorisé. Si l'environnement des télécommunications n'est pas suffisamment sécuritaire pour garantir la confidentialité, les données sociosanitaires nominatives communiquées devront être encryptées avant leur expédition et désencryptées à leur arrivée seulement (chiffrement).

9. Mandat confié par un organisme à une personne ou à un autre organisme

Tout mandat confié par un organisme à une personne ou à un autre organisme doit se faire par écrit. Le mandant verra en outre :

- à préciser clairement dans le texte de l'entente les objectifs et les finalités du mandat, les modalités de communication...;

- à faire signer au mandataire une clause de respect de confidentialité;

- à obliger les mandataires à garantir la protection des données sociosanitaires qu'ils recevront, à ne pas s'en servir pour leurs fins propres, à sensibiliser et à former les membres de leur personnel à cet égard;

- à tenir les mandataires responsables si leur personnel contrevient à la *Loi sur l'accès*;

- à inclure une clause de cessation du contrat ou du service avec le mandataire si ce dernier contrevient aux obligations prévues dans l'entente ou à la *Loi sur l'accès*;

- à faire en sorte qu'un fournisseur de services ayant reçu un mandat voit à ce que les autres fournisseurs à qui il fait lui-même appel se conforment aux exigences du mandat;

- à ce que le mandataire lui retourne ou détruise les renseignements obtenus lorsque son mandat a été complété ou annulé et ce, peu importe la raison.

10. Partage de bases de données communes ou d'un centre de traitement commun

Si plusieurs organismes ont à partager les mêmes bases de données ou le même centre informatique pour le traitement des données sociosanitaires, ils doivent prendre toutes les mesures nécessaires afin qu'aucun des autres organismes n'ait accès à leurs données respectives sans le consentement de l'usager.

11. Programme de sensibilisation et d'embauche de personnes

- La sélection du personnel ayant accès aux données nominatives des usagers doit se faire avec un grand discernement.

- Les organismes feront signer une clause de respect de la confidentialité au personnel qui a accès aux données sociosanitaires (cette règle vaut pour toute personne extérieure à l'organisme qui a accès à ce type de données).

- Les organismes doivent sensibiliser et former leur personnel à la nécessité de protéger la confidentialité des données sociosanitaires (en transmettant périodiquement sur les écrans des utilisateurs des messages de protection des données sociosanitaires, en mettant des affiches de non-divulgation, etc.).

- Les organismes doivent éduquer les utilisateurs à clore leur session de travail lorsqu'ils quittent leur poste de travail.

- Les organismes prévoiront des mesures disciplinaires (pouvant aller jusqu'au congédiement) pour toute contravention à l'intégrité des données sociosanitaires ou à leur divulgation.

12. Communication de données sociosanitaires

Pour communiquer des données sociosanitaires, il faut obtenir le consentement de la personne concernée ou encore satisfaire aux conditions prévues par la *Loi sur les services de santé et les services sociaux*.

- Le récipiendaire doit disposer de mesures de protection adéquates.
- Seules les données nécessaires doivent être communiquées.

- Dans les cas de communication à des fins d'étude, de recherche ou de statistique, les organismes doivent s'assurer de la nécessité de communiquer des données sous forme nominative; sinon, ils verront à les dénominaliser avant de les communiquer au chercheur. Ce dernier doit en outre s'engager par écrit à traiter ces données de façon confidentielle et à les détruire après utilisation.

13. Les micro-ordinateurs

- Utiliser un logiciel d'accès pour les micro-ordinateurs du genre « Sesame » (produit québécois).
- Pour empêcher les infections informatiques, certaines mesures doivent être prises :
  - ne jamais utiliser des programmes ou des logiciels de provenance douteuse ou extérieure à l'organisme;
  - sensibiliser les utilisateurs aux dangers d'infections informatiques;
  - mettre en place des procédures d'audit informatique et de contrôle de logiciels;
  - utiliser des programmes de prévention et des fonctions de sécurité (contrôler l'accès logique aux stations de travail, chiffrer les données...).
- ˜Désactiver la clé « Print screen » lorsque des données nominatives apparaissent à l'écran afin d'éviter des impressions de dossiers sans autorisation.

14. Impression des données sociosanitaires

- Le droit d'un utilisateur d'imprimer des données sociosanitaires doit faire l'objet d'une politique approuvée par la haute direction. Cette politique doit également prévoir les modalités de disposition des imprimés après leur utilisation.
- L'impression de ces documents doit se faire par des utilisateurs et dans des lieux autorisés.

15. Délai d'implantation

- La Commission d'accès à l'information accorde aux organismes un délai de trois ans afin d'adapter leurs systèmes existants à ces exigences minimales.
- La Commission demande que les systèmes en développement soient conformes à ces exigences minimales dès leur implantation.

16. Non-respect de certaines normes

À cause de la multitude d'équipements et de logiciels utilisés dans le réseau de la Santé et des Services sociaux, il se peut qu'une norme décrite dans ce document soit techniquement inapplicable; dans ce cas, la Commission demande à l'organisme concerné d'introduire dans son plan directeur les ressources nécessaires pour modifier ses équipements ou pour concevoir des programmes d'appoint.

CONCLUSION

Nous avons présenté les mesures de sécurité minimales à instaurer dans les systèmes informatiques pour gérer les dossiers des usagers du réseau de la Santé et des Services sociaux.

Ces mesures de sécurité doivent être énoncées dans des procédures administratives écrites par chaque établissement.

Un organisme public peut évidemment adopter des mesures de sécurité supplémentaires ou plus strictes, de façon à bien protéger les renseignements confidentiels qui lui sont confiés.

M. Benoît Elie et Mme Alice Labrèque sont les auteurs de ce document et ont aussi procédé aux consultations étendues dont il a fait l'objet.

M. Elie et Mme Labrèque tiennent à souligner la participation importante de M. Claude Francoeur au projet préliminaire de politique publié en août 1991.