

AVIS CONCERNANT
LE SYSTÈME DE GESTION
DES DEMANDES D'ÉVALUATION
DU BUREAU D'ÉVALUATION MÉDICALE
DU MINISTÈRE DU TRAVAIL

DOSSIER 01 18 22

AVRIL 2002

TABLE DES MATIÈRES

INTRODUCTION	1
1. PORTÉE DE L'ÉVALUATION	1
2. DESCRIPTION DU PROJET	2
3. ÉVALUATION DU PROJET.....	2
3.1 La responsabilité.....	2
3.2 La confidentialité des renseignements personnels lors de la transmission.....	2
3.3 La journalisation des accès	4
3.4 L'entrepôt de données	4
3.5 La conservation des renseignements personnels dans la base de données	5
CONCLUSION	6

INTRODUCTION

Sous la responsabilité du sous-ministre adjoint des relations du travail au ministère du Travail du Québec (Ministère), le Bureau d'évaluation médicale (BEM) veille à l'application du mécanisme d'évaluation médicale prévu dans la *Loi sur les accidents du travail et les maladies professionnelles* (articles 216 à 225). Ce Bureau a pour fonction de donner un avis afin de confirmer ou d'infirmer les conclusions du médecin qui a charge du travailleur ou du médecin désigné par la Commission de la santé et de la sécurité du travail (CSST) ou l'employeur. On fait appel au BEM lorsqu'il y a contestation d'une question d'ordre médicale, par l'employeur ou par la CSST (articles 206 et 212) ou lorsque cette dernière désire un avis médical même s'il n'y a pas de contestation (article 204).

Les avis émis par les membres du BEM lient la CSST qui doit rendre une décision en conséquence. Le BEM s'assure que les avis produits par ses membres sont conformes à la loi et émis dans les délais qui y sont prévus.

Le BEM possède deux places d'affaires, soit le 200, chemin Sainte-Foy, à Québec et le 35, Port-Royal Est, à Montréal. Le nombre de ses ressources humaines est respectivement de 5 à Québec et de 12 à Montréal. À ces ressources se greffe un groupe de médecins (les membres) chargés de faire les évaluations médicales, au cœur de la mission du BEM. Le nombre de membres est actuellement de 82. Finalement, quatre pneumologues siègent au Comité des maladies pulmonaires professionnelles (CMPP).

Le volume total de dossiers traités annuellement est d'environ 10 500 dossiers (9 200 évaluations, 570 avis complémentaires et 670 dossiers du CMPP). Les deux tiers de ces dossiers sont traités par le bureau de Montréal.

1. PORTÉE DE L'ÉVALUATION

Le projet de développement du système du BEM qui est présenté à la Commission prévoit trois phases, soit le remplacement du système actuel, l'ajout de nouvelles fonctionnalités et la mise en place d'un lien électronique bidirectionnel entre la CSST et le BEM. Le Ministère demande un avis sur les deux premières phases du projet. La troisième phase fera l'objet d'une demande d'avis distincte suite à la mise à jour des architectures et à la définition des mécanismes d'échanges d'information prévue entre les phases II et III.

L'évaluation repose principalement sur les informations contenues dans les documents qui nous furent transmis par le Ministère et sur des entrevues effectuées auprès des responsables désignés du Ministère.

Les mesures de sécurité ont été questionnées, cependant la technologie utilisée n'a pas fait l'objet d'une évaluation technique et la sécurité en place n'a pas fait l'objet de corroboration.

2. DESCRIPTION DU PROJET

Le projet consiste en une refonte du système actuel de gestion des demandes d'évaluation médicale auquel seront intégrés le suivi des dossiers et le suivi des avis complémentaires. De plus, un entrepôt de données sera mis en place pour faciliter l'exploitation des données par l'utilisateur et de nouvelles fonctionnalités seront ajoutées pour supporter plus efficacement les processus d'affaires.

Le nouveau système sera développé selon les orientations technologiques du Ministère, soit une base de données « *Oracle* », les outils de développement « *Forms* » et « *Report* » ainsi que l'atelier intégré de génie logiciel (AIGL) de la compagnie Oracle. Le système sera déployé et exploité sur l'infrastructure existante du réseau du Ministère. La saisie des données se fera au 35, Port-Royal Est, à Montréal et au 200, chemin Sainte-Foy, à Québec, tandis que le « stockage » et le traitement des données seront centralisés à Québec, au 800, place d'Youville. Le système du BEM utilisera les infrastructures de télécommunications du Ministère qui sont constituées, entre autres, de liens sur le Réseau intégré des communications informatiques et bureautiques (RICIB).

3. ÉVALUATION DU PROJET

3.1 La responsabilité

Tout organisme public est responsable d'assurer la protection des renseignements personnels dont il a la gestion.

La Commission considère important l'implication et la participation du responsable de la protection des renseignements personnels, et ce, dès les premières phases de la conception d'un projet informatique impliquant des données nominatives. Ses connaissances des principes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., chap. A-2.1, ci-après appelée *Loi sur l'accès*) peuvent contribuer à en assurer l'application.

3.2 La confidentialité des renseignements personnels lors de la transmission

Les responsables du Ministère mentionnent que les données du BEM sont conservées sur un serveur unique dans un lieu sécurisé et dont les accès physiques et logiques sont contrôlés. Ils mentionnent également que les tables de données du BEM sont indépendantes de celles du Ministère.

Le nouveau système sera déployé et exploité sur l'infrastructure existante du réseau du Ministère, au 800, place d'Youville. Ceci implique que le système du BEM utilisera les infrastructures de télécommunications du Ministère qui sont constituées, entre autres, de liens sur le RICIB.

Le nouveau système implique la création d'une base de données accessible par les employés autorisés du BEM à partir du bureau situé au 35, Port-Royal Est, à Montréal et au 200, chemin Sainte-Foy, à Québec. Le « stockage » et le traitement des données seront centralisés à Québec, au 800, place d'Youville. Ceci implique que les données personnelles (données à caractère médical sur des travailleurs) seront transférées par l'infrastructure de télécommunications du RICIB.

Dans un tel contexte, comment assurer le caractère confidentiel des renseignements? À cet effet, il faut considérer les éléments suivants.

Le comité de travail du Conseil du trésor concernant la gestion de la sécurité de l'information dans l'administration québécoise souligne :

« Au fur et à mesure que les extranets, les intranets et les serveurs Web s'imposent au sein des organisations, il devient nécessaire de sécuriser davantage ce nouvel environnement ouvert ainsi que l'information qui y circule. »¹

La Commission d'accès à l'information recommandait dans son rapport sur la sécurité des renseignements personnels :

« Utiliser des techniques de cryptographie pour la transmission de données sensibles, confidentielles et stratégiques. »²

Par ailleurs, la *Loi concernant le cadre juridique des technologies de l'information* énonce :

« Lorsque la Loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication. »³

¹ Rapport du comité de travail gouvernemental sur la sécurité de l'information, avril 1999.

² Rapport sur la sécurité et la confidentialité des renseignements personnels dans l'appareil gouvernemental, octobre 1998.

³ Article 34 de la *Loi concernant le cadre juridique des technologies de l'information*.

Enfin, dans le document intitulé « *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux*, la Commission a précisé :

« 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). »

Compte tenu de ce qui précède, la Commission est d'avis que le Ministère doit garantir la confidentialité, lors de la transmission des renseignements personnels, par le chiffrement des informations.

3.3 La journalisation des accès

Faisant suite aux discussions avec les responsables du Ministère concernant la journalisation des accès, ces derniers nous confirment leur engagement à mettre en place les mécanismes suivants :

« Le ministère mettra en place des mécanismes de base permettant de consigner chaque consultation et mise à jour des informations nominatives en conservant, entre autres, des données telles que la personne ayant accédé aux données, la date et l'heure de l'accès, le type d'accès ainsi que le dossier consulté. Cette façon de faire permettra au ministère, d'identifier toute information nécessaire reliée à l'exploitation du système. »⁴

La Commission considère que la journalisation des accès permet de contrôler l'utilisation de l'information et de s'assurer que seuls les employés autorisés ont accès aux informations pertinentes à leur fonction. Toute fuite de renseignements personnels est par conséquent plus facile à détecter et à évaluer dans le cas d'une intrusion ou d'une fraude. De plus, une analyse des données journalisées devrait être effectuée afin d'identifier les accès non autorisés à des renseignements personnels.

3.4 L'entrepôt de données

⁴ Document demande d'avis à la Commission du 5 mars 2002, p.10.

La mise en place d'un entrepôt de données exploitables directement par les utilisateurs fait partie des orientations du Ministère. Les responsables du Ministère mentionnent que cette façon de faire permettra à la Direction des ressources informationnelles de diminuer les efforts à consacrer au développement de rapports opérationnels et « *ad hoc* » et de permettre à l'utilisateur de bénéficier d'une autonomie quant à l'exploitation de ses propres données.

Les données seront sur un serveur isolé et l'accès sera limité à deux personnes du BEM, une à Montréal et une autre à Québec.

La Commission met en garde le Ministère quant à la réplique des données puisque cette avenue requiert une rigueur accrue des accès, du transfert et de la conservation des renseignements personnels de par la gestion de deux bases de données. Cette façon de procéder nécessite une attention particulière au maintien de l'exactitude des données par des mécanismes de synchronisation lors de la mise à jour des informations aux deux bases de données. À cet égard, il y a lieu de rappeler l'article 72 de la Loi d'accès qui édicte que :

72. Un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis.

3.5 La conservation des renseignements personnels dans la base de données

Le dossier physique (dossier médical, formulaire et avis) est conservé selon le calendrier de conservation approuvé, soit un an actif, deux ans semi-actif, puis détruit.

Toutefois, le calendrier de conservation est muet quant aux renseignements déposés dans la base de données du Ministère. Le calendrier du BEM n'a pas été modifié pour y inclure la conservation des données informatisées.

En l'absence de prescription quant à la détention des données informatisées, il faut considérer ce que prévoit l'article 73 de la Loi sur l'accès :

73. Lorsque l'objet pour lequel un renseignement nominatif a été recueilli est accompli, l'organisme public doit le détruire, sous réserve de la Loi sur les archives (chapitre A-21.1).

Ainsi, en vertu de cet article, le BEM pourrait détenir les données nominatives informatisées aussi longtemps que n'est pas accompli l'objet pour lequel elles ont été recueillies et non pas sur une base permanente.

CONCLUSION

La Commission veut s'assurer de la protection des renseignements personnels qui sont transmis sur les réseaux de télécommunications gouvernementaux, plus spécifiquement dans des environnements de plus en plus ouverts. Par conséquent, l'exigence de chiffrement des données nominatives lors de leur transmission s'avère une exigence minimale d'autant plus lorsqu'il s'agit de renseignements à caractère médical.

Par ailleurs, la Commission considère que l'accessibilité aux renseignements personnels contenus dans les bases de données doit être journalisée afin de contrôler les accès uniquement aux personnes autorisées et de pouvoir, s'il y a lieu, faire les vérifications qui s'imposent.

Enfin, le Ministère doit, en regard des renseignements personnels contenus dans les bases de données, appliquer des règles de conservation qui ne permettent pas une détention permanente des informations.