LOI 25 SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

DE NOUVELLES OBLIGATIONS POUR LES CLINIQUES

Élyanthe Nord

Me Cynthia Chassigneux

La première échéance arrive bientôt : le 22 septembre. Ce jour-là, de nouvelles obligations incomberont aux cliniques concernant la protection des renseignements personnels. Il s'agit de mesures imposées par la loi 25, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, adoptée il y a un an.

Que faut-il faire d'ici cette date ? La clinique, comme toute entreprise privée, doit, tout d'abord, nommer un responsable de la protection des renseignements personnels. Une personne qui gérera toutes les informations liées aux patients, mais aussi à ses employés.

« La loi indique que c'est la personne détenant la plus haute autorité au sein de l'entreprise – ou du cabinet – qui est de facto responsable de la protection des renseignements personnels. Elle peut toutefois déléguer cette fonction », explique **Me Cynthia Chassigneux**, avocate spécialisée en protection des renseignements personnels et associée chez Langlois Avocats, à Montréal.

Le responsable de la protection des renseignements personnels devra veiller à l'application et au respect de la loi au sein du cabinet médical. C'est lui qui aura notamment la tâche de gérer les incidents de confidentialité, de s'assurer que toutes les échéances concernant les nouvelles mesures prévues par la loi soient respectées et de mettre sur pied un registre des incidents.

Ce travail peut-il être confié à une adjointe administrative ? « Il n'y a pas de profil type de la personne responsable. Cependant, idéalement, elle doit très bien connaître le cabinet médical, posséder des connaissances en matière de protection des renseignements personnels et disposer d'une certaine autorité pour que toutes les mesures qui devront être mises en œuvre le soient. Cette personne peut éventuellement être une secrétaire ou une adjointe à qui l'on donnera toute la latitude nécessaire », explique l'avocate, qui a été six ans juge à la Commission d'accès à l'information.

Plusieurs possibilités, parfois inattendues, s'offrent par ailleurs aux cliniques. La gestion des renseignements personnels peut ainsi être confiée à l'extérieur, par exemple, à une firme d'avocats. Des cabinets médicaux peuvent aussi se regrouper et n'avoir qu'un seul responsable.

Dix ou vingt groupes de médecine de famille (GMF) pourraient-ils se partager les services d'un unique mandataire ? « Rien dans la loi ne les en empêche, indique Me Chassigneux, titulaire d'un doctorat et d'un postdoctorat en droit. Il n'y a pas de limite pour l'instant. Ces obligations sont toutes nouvelles pour les entreprises. On est encore un peu dans le flou. Mais est-ce souhaitable qu'une seule personne s'occupe de dix cliniques ? »

Le responsable devra entre autres se charger des demandes liées aux renseignements personnels. Il aura ainsi à répondre aux patients qui veulent avoir accès à leur dossier médical, aux employés du cabinet qui désirent des informations et, éventuellement, en cas de plaintes ou de problème de confidentialité, à la Commission d'accès à l'information, un organisme dont les pouvoirs ont été renforcés par la loi 25.

Une fois le responsable des renseignements personnels désigné, son titre et ses coordonnées doivent être inscrits sur le site Internet de la clinique. Si le cabinet ne possède pas de site, il peut utiliser un autre moyen. Par exemple, mettre les informations sur une affiche dans la salle d'attente ou à la réception.

INCIDENTS DE CONFIDENTIALITÉ

D'autres obligations attendent les cabinets médicaux le 22 septembre prochain. En cas « d'incident de confidentialité », ils devront dorénavant prendre plusieurs mesures.

« Qu'entend-on par incident de confidentialité ? Il s'agit de tout ce qui est lié à l'obtention, à l'utilisation, à la communication non autorisées d'un renseignement personnel, d'un fichier comportant plusieurs informations personnelles ou, dans le cas d'une clinique, d'un dossier. Il ne s'agit pas seulement des

dossiers des patients, mais aussi de ceux du personnel de la clinique », précise Me Chassigneux.

Des exemples d'incidents de confidentialité : un dossier médical ou des résultats d'analyse transmis à la mauvaise personne, l'envoi d'un relevé T4 à un employé à qui il n'appartient pas, la perte de données d'un patient, la consultation d'un dossier médical par une personne non autorisée. Certains cas peuvent être très graves : l'envoi de tous les dossiers de la clinique au mauvais endroit, la divulgation malencontreuse de résultats de tests qui deviennent publics, etc. « C'est vraiment de toutes ces possibilités qu'il va falloir se protéger. Certains risques peuvent maintenant être accrus à cause du télétravail où l'on passe du bureau à la maison avec notre ordinateur. »

À partir du 22 septembre, en cas d'incident de confidentialité, les cliniques devront :

1) évaluer le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements personnels sont touchés par l'incident ;
2) prendre les mesures raisonnables pour diminuer les risques de préjudice et éviter que de nouveaux incidents de même nature ne se produisent ;
3) aviser la Commission d'accès à l'information et la personne concernée si l'incident présente un risque de préjudice sérieux.
4) tenir un registre des incidents dont la Commission d'accès à l'information pourra demander une copie.

Comment évaluer si une violation de la confidentialité présente « un risque de préjudice sérieux » ? Il faut effectuer une analyse des menaces liées à la sensibilité des renseignements touchés. « Si seuls le nom et le prénom sont divulgués dans un cabinet généraliste, ce n'est pas trop grave, mentionne l'avocate. S'il s'agit d'une clinique spécialisée, cela commence à devenir un peu plus délicat. Si des analyses médicales, des résultats en pathologie, des prescriptions ou tout le dossier médical sont communiqués ou diffusés, là ça devient vraiment plus problématique. Si, en plus, des renseignements comme le numéro d'assurance maladie sont dévoilés, l'incident peut être encore plus préjudiciable. »

Divers scénarios peuvent se produire. Si, par exemple, un patient a reçu des résultats qui ne lui étaient pas destinés, dans le meilleur des cas, il avertit la clinique. « On peut alors lui faire signer une déclaration mentionnant qu'il va les effacer de tous les supports sur lesquels il les a acquis. S'il les a eus par courriel, on lui demande de s'engager à l'éliminer, d'indiquer qu'il n'a jamais enregistré les résultats et qu'il ne s'en servira pas. La clinique prend ainsi plusieurs mesures lui permettant de montrer qu'elle a agi pour circonscrire les risques d'atteinte. »

ENCADRÉ 1 | QU'EST UN PRÉJUDICE SÉRIEUX ?

Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple :

- à l'humiliation ;
- à une atteinte à la réputation ;
- à une perte financière ;
- à un vol d'identité ;
- à des conséquences négatives sur un dossier de crédit ;
- à une perte d'emploi.

Source : Site du Gouvernement du Québec, *https://bit.ly/incident-confidentialité-gouv*

Si un employé reçoit le mauvais relevé T4, la gestion de la situation est la même. « Cela dépend de ce qu'il va faire du document. Est-ce qu'il va le diffuser ? Est-ce qu'il va porter atteinte à la réputation de son collègue ? En général, si l'on est capable de récupérer l'information, le préjudice va être moindre. »

PLAN D'ACTION

Vers qui se tourner quand survient un incident de confidentialité, quel qu'il soit ? Pour parer à toute éventualité, il est conseillé d'avoir une liste de personnes-ressources. La cellule de crise peut comporter, outre le responsable des renseignements personnels du cabinet, un informaticien au cas où la violation de confidentialité relève de l'informatique, mais également un avocat spécialisé en protection des renseignements personnels. « Il pourra faire une analyse de risque et évaluer les conséquences appréhendées pour la personne touchée (*encadré 1*). Il permettra aussi à la clinique de prendre les mesures nécessaires pour documenter les actions prises et préserver les preuves », affirme Me Chassigneux. Il faut aussi avoir sous la main les coordonnées de son assureur. « On doit savoir si l'on est assuré ou non pour l'incident de confidentialité. »

La Commission de l'accès à l'information, pour sa part, propose plusieurs étapes quand survient un incident de sécurité (*https://bit.ly/incident-sécurité*) :

- déterminer rapidement les causes de l'incident ;

ENCADRÉ

AUTRES RÈGLES À PARTIR DU 22 SEPTEMBRE

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* imposera également sous peu des règles particulières qui touchent les cliniques.

RECHERCHE

À partir du 22 septembre, la communication des informations personnelles sans le consentement de la personne concernée sera encadrée par de nouvelles règles, notamment dans le cas d'études, de recherches et de la production de statistiques. « Lorsqu'un étudiant ou un chercheur demandera à un cabinet l'autorisation d'étudier ses dossiers médicaux, une évaluation des facteurs relatifs à la vie privée sera nécessaire. En outre, une entente devra être signée entre le cabinet et le chercheur », indique Me Cynthia Chassigneux.

TRANSACTIONS COMMERCIALES

Que se passera-t-il après le 22 septembre dans le cas d'une fusion de deux cabinets ou de la vente d'une clinique ? Les acheteurs ou les partenaires pourront-ils avoir accès aux dossiers médicaux ? « L'article 18.4 indique que cela pourra être fait, mais que les parties devront conclure une entente, dont la loi 25 stipule les éléments, précise l'avocate. Le secret professionnel doit par ailleurs demeurer. »

MESURES BIOMÉTRIQUES

La loi 25 prévoit également des mesures concernant le recours à la biométrie. Et certaines s'appliquent déjà. Ainsi, la création d'une banque de caractéristiques ou de mesures biométriques doit être divulguée à la Commission d'accès à l'information au plus tard 60 jours avant sa mise en service. Si une clinique décidait de demander à ses employés de donner, à partir du 22 septembre, leur empreinte digitale plutôt que d'utiliser une carte magnétique pour entrer au bureau, il faudrait donc qu'elle en ait déjà fait part le 22 juillet, en vertu de la *Loi concernant le cadre juridique des technologies de l'information* que la loi 25 est venue aussi moderniser.

- mettre fin à la fuite ;
- informer les personnes visées ;
- déclarer l'incident à la Commission ;
- prendre les mesures nécessaires pour diminuer les conséquences préjudiciables que sont susceptibles de subir les personnes touchées ;
- mettre en place les mesures requises pour éviter qu'un tel incident ne se reproduise.

TRAVAIL PRÉPARATOIRE CONSEILLÉ PAR LA COMMISSION

D'ici le 22 septembre, les cliniques doivent donc bien se préparer. La Commission recommande notamment plusieurs mesures :

- FAIRE L'INVENTAIRE DES RENSEIGNEMENTS PERSONNELS

  Chaque cabinet médical devrait répertorier les informations personnelles qu'il conserve et en évaluer la sensibilité. « Cet exercice permet d'avoir une vue d'ensemble des renseignements que l'on détient au cas où un incident arrive, explique Me Chassigneux. Si on sait que le serveur touché contenait les données du service de paye ou tous les dossiers médicaux, on agira le plus vite possible. »

- METTRE EN PLACE DES MESURES POUR PRÉVENIR OU LIMITER LES CONSÉQUENCES D'UN INCIDENT DE CONFIDENTIALITÉ

  « Le cabinet médical doit se demander quelles mesures de sécurité ont été mises en place autant vis-à-vis de l'interne que vis-à-vis de l'externe », mentionne l'avocate. La clinique doit ainsi vérifier avec son service informatique les précautions prises. « A-t-on des pare-feu ? Fait-on régulièrement des tests d'intrusion ? » Si les données ne sont pas stockées dans le centre médical, il faut voir avec l'hébergeur quelles sont ses mesures de sécurité. « On est responsable des renseignements que l'on détient, mais aussi de ceux que l'on confie à l'externe », souligne Me Chassigneux.

  Un travail de sensibilisation doit également être fait auprès du personnel. Les failles découlent très souvent d'un facteur humain. « Rappelle-t-on aux employés les règles en matière de communication et d'utilisation des renseignements personnels ? Il est aussi important de répéter, par exemple, que lorsque l'on quitte son ordinateur pour aller manger, il faut fermer sa session afin que personne ne puisse y avoir accès. Le soir, les dossiers papier doivent être rangés, les classeurs fermés ou la pièce dans laquelle ils se trouvent, verrouillée. Le papier existe encore. »

  Il faut, par ailleurs, que les employés sachent que si jamais ils sont à l'origine d'un incident de confidentialité ou en sont témoins, ils ne doivent pas hésiter à prévenir le responsable de la protection des renseignements personnels. Ce dernier pourra alors prendre les mesures nécessaires pour réduire les risques.

  Ces différentes démarches doivent ensuite être mises par écrit. « Il faut tout documenter pour montrer le cas échéant que le cabinet médical a agi de manière responsable », conseille Me Chassigneux.

- INSTAURER DES PRATIQUES PERMETTANT DE RÉAGIR ADÉQUATEMENT ET RAPIDEMENT
  La Commission recommande d'avoir des outils pour agir immédiatement en cas d'incident de confidentialité, comme un plan de réponse aux incidents et des directives à l'intention des employés.

  On doit, par ailleurs, se préparer à plusieurs scénarios : faille informatique, hameçonnage, erreur d'un employé, indiscrétion, entrée intrusive, etc. « Il faut prévoir des mesures pour réagir sur le plan technique et organisationnel », indique Me Chassigneux.

AUTRES ÉCHÉANCES : SEPTEMBRE 2023 ET 2024

La loi 25 comporte également des dispositions qui entreront en vigueur en septembre 2023 et 2024. Ainsi, dans un an, les entreprises privées, dont les cliniques, devront avoir établi des politiques encadrant la gouvernance des renseignements personnels et en publier des informations détaillées sur leur site Internet. Il leur faudra également respecter de nouvelles règles dans différents domaines : l'utilisation de renseignements personnels, le consentement, etc. Les cabinets devront en outre détruire les informations personnelles lorsque « la finalité de leur collecte est accomplie » ou les anonymiser. Le site de la Commission indique en particulier une douzaine de futures mesures.

RESPONSABILISER LES ENTREPRISES

Pourquoi tout à coup cette modernisation des lois sur les renseignements personnels ? Des provinces comme l'Alberta et la Colombie-Britannique obligent depuis déjà longtemps les entreprises à déclarer les incidents de confidentialité, affirme Me Chassigneux. « Au Québec, la Commission d'accès à l'information demandait de telles mesures depuis plus de dix ans. Et puis, en 2019, il y a eu cette institution financière qui a été victime d'un incident de confidentialité qui a touché 9,7 millions de personnes. » Le but de la loi 25 était donc de responsabiliser les entreprises concernant la protection des renseignements personnels qu'elles détiennent et d'encadrer la manière dont elles en assurent la sécurité.

Pour plus d'informations, consulter le guide sur les nouvelles responsabilités des entreprises, les pistes d'action et les bonnes pratiques : *https://bit.ly/guide-nouvelles-responsabilités-entreprises.* //

WEBINAIRE SUR LA LOI 25 LE 7 SEPTEMBRE 2022

La formation « Loi 25 – Modernisation de la protection des renseignements personnels. Quelles sont les répercussions sur mon cabinet ? » sera donnée par Me Cynthia Chassigneux.
https://bit.ly/activités-formations-webinaires