EMOND HARNDEN
LABOUR & EMPLOYMENT LAW
DROIT DU TRAVAIL ET DE L'EMPLOI

# Le CIPVP ordonne à un hôpital de prendre des mesures de protection des données

février 3, 2015

Le 16 décembre 2014, le Commissaire à l'information et à la protection de la vie privée (« CIPVP ») de l'Ontario a rendu l'ordonnance HO-013, en application de la LPRPS, enjoignant le Rouge Valley Health System (« Hôpital ») à mettre en œuvre plusieurs mesures de protection des données. L'ordonnance fait suite à un examen par le CIPVP de la gestion des renseignements médicaux personnels par l'Hôpital. Cet examen découle de rapports selon lesquels il y a eu consultation et divulgation non autorisées de renseignements médicaux personnels de nouvelles mères qui étaient des patientes à l'Hôpital. Le CIPVP a conclu que les mesures de protection en place à l'Hôpital étaient inadéquates et a émis plusieurs directives afin de remédier aux lacunes. L'ordonnance rendue par le CIPVP visait uniquement le Rouge Valley Health System, mais toutes les institutions de soins de santé devraient prendre connaissance des directives du CIPVP et examiner leurs propres systèmes de protection des données afin de garantir qu'ils sont conformes aux obligations prescrites par la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (« Loi »), comme l'énonce l'ordonnance HO-013.

Le CIPVP a entamé son examen après que l'Hôpital a présenté deux rapports d'atteinte à la vie privée de patientes. Même si les deux incidents étaient distincts et non liés, ils mettaient en cause des employés de l'Hôpital occupant des postes administratifs qui ont consulté et divulgué des renseignements médicaux personnels de mères qui avaient récemment donné naissance, afin qu'on puisse leur vendre ou leur proposer des régimes enregistrés d'épargne-études. Au cours de son examen, le CIPVP a constaté que l'Hôpital ne disposait pas de suffisamment de mesures techniques et administratives pour protéger les renseignements médicaux personnels de ses patients et que les employés de l'Hôpital n'avaient pas été suffisamment formés et sensibilisés en matière de protection de la vie privée. Le CIPVP a donné les directives suivantes à l'Hôpital :

- Veiller à ce que le système informatique, dans lequel il stocke les renseignements médicaux personnels de ses patients, puisse vérifier tous les cas d'accès aux renseignements sur les patients.
- Veiller à ce que l'Hôpital puisse accéder, aux fins de vérification, au registre des activités des utilisateurs à l'égard du système informatique.
- Limiter les capacités de recherche et les fonctionnalités du système informatique de manière à ce que les employés soient incapables d'effectuer des recherches illimitées de renseignements médicaux personnels et puissent seulement effectuer ces recherches au moyen des critères suivants :
    - numéro de carte d'assurance santé;
    - numéro de dossier médical;

    - numéro de consultation;
    - prénom exact, nom de famille et date de naissance.
- Passer en revue et réviser ses politiques en matière de protection de la vie privée pour appliquer les conclusions figurant dans l'ordonnance.
- Élaborer et mettre en œuvre des politiques relatives à la formation et à la sensibilisation en matière de protection de la vie privée et à la gestion des atteintes à la protection des données.
- Passer en revue et réviser ses outils et documents de formation en matière de protection de la vie privée pour appliquer les conclusions figurant dans l'ordonnance.
- Donner une formation sur la vie privée à tous les employés de l'Hôpital – immédiatement pour ceux qui occupent des postes administratifs et, pour les autres employés, au plus tard le 16 juin 2015.

La plupart des hôpitaux et des organismes de soins de santé ont en place des politiques et des mesures de protection contre les atteintes à la vie privée. Le risque d'atteinte est constant dans le secteur des soins de santé, de sorte que les organismes doivent porter une attention particulière aux mesures qu'ils prennent pour protéger les renseignements médicaux personnels en leur possession. Comme nous l'avons vu au cours de la dernière année, les pertes et les vols de données fortement médiatisés démontrent l'importance de ces mesures pour remédier aux risques d'accès non autorisés à des renseignements médicaux personnels à partir de l'extérieur de l'organisme et de perte de possession de ces renseignements.

L'ordonnance HO-013 démontre à quel point il est important qu'un organisme prenne des mesures pour remédier aux atteintes internes à la vie privée. Les conséquences pour le Rouge Valley Health System dans cette affaire ne se sont pas limitées à une ordonnance défavorable du CIPVP. Une demande de recours collectifs a été présentée contre Rouge Valley Health System au nom des patientes qui ont subies une atteinte à leur vie privée, ce qui pourrait également entraîner une perte financière.

L'ordonnance HO-013 donne des indications utiles concernant le degré et l'ampleur des mesures qui seront nécessaires afin de conférer une protection raisonnable contre les atteintes internes à la vie privée. Bien que la conformité aux lignes directrices formulées par le CIPVP dans l'ordonnance HO-013 ne garantisse pas que l'organisme évitera toute responsabilité, il s'agit d'un pas important dans la direction d'une gestion efficace des risques découlant de son traitement des renseignements médicaux personnels.

Si vous avez des questions au sujet de l'ordonnance HO-013 ou si vous voulez discuter des mesures que votre organisme pourrait prendre afin de protéger les renseignements personnels en sa possession et gérer le risque d'atteinte, veuillez communiquer avec Sarah Lapointe au 613-940-2738.