Can J Anesth/J Can Anesth (2020) 67:163–168
https://doi.org/10.1007/s12630-019-01532-3

EDITORIALS

Understanding privacy risks when accessing electronic medical records

Daniel Tardif, MD, LMCC, MBA, CHRP/CRHA, CCPE

Received: 19 August 2019 / Revised: 27 September 2019 / Accepted: 1 October 2019 / Published online: 2 December 2019

The Canadian healthcare sector continues to see an increase in use of technologies for managing personal health information (PHI), with the majority of healthcare providers now substituting their paper files for electronic medical records (EMR).[1]

Modern healthcare requires inter-professional collaboration and coordination. This is particularly important in a hospital setting where one patient typically receives care from a variety of individuals such as emergency room physicians, surgeons, anesthesiologists, and nurses, among others. Electronic medical record systems facilitate the provision of modern healthcare by allowing large volumes of PHI to be stored and shared among individuals.[2]

While shared EMR offer significant benefits, such as easier exchange of information to provide timely and quality care, they also pose unique privacy risks. The same general requirements for privacy apply for both paper and electronic medical records, but the possibility for an EMR to be accessed by a large number of users and the wide access that is possible from multiple locations are two examples of how this improved record keeping method presents new risk management challenges. These risks have been highlighted in a number of cases where privacy breaches occurred because of unauthorized access of EMRs to view, use, or disclose PHI.[3,4] Although unauthorized access can be motivated by financial or personal interests, it can also arise from an innocent misunderstanding of one's privacy obligations.

D. Tardif, MD, LMCC, MBA, CHRP/CRHA, CCPE (✉)
Canadian Medical Protective Association, 875 Carling Avenue, Ottawa, ON, Canada
e-mail: privacyoffice@cmpa.org

In Canada, the collection, use, and disclosure of PHI is governed by a patchwork of federal, provincial, and territorial statutes.[5] Medical regulatory authorities (i.e., provincial "colleges") also have numerous relevant policies, bylaws, rules, and regulations. Privacy obligations can be difficult to navigate given the evolving legislative and regulatory frameworks. The frameworks also vary across Canada, so it is important for physicians to understand the specific requirements applicable where they practice.

The Canadian Medical Protective Association frequently receives calls from physicians seeking medical-legal advice or assistance related to EMRs and privacy issues. This article provides general comments in an effort to clarify privacy obligations in this context, including who can access EMRs to view, use, or disclose PHI, and for what purposes.[A]

Accessing EMRs to view, use, or disclose PHI

Role of health information custodians

A health information custodian (HIC)[B] is an entity that has control over PHI in its custody. Hospital administrators and clinic owners are typical examples of HICs for PHI stored within their facilities.[C] These HICs are responsible to collect, use, or disclose PHI in accordance with the applicable legislative and regulatory framework. This includes taking measures to prevent unauthorized access, use, and disclosure of PHI.[6]

The HIC can designate agents[D] to act on their behalf and fulfill their privacy obligations.[6] Where the hospital is the HIC, agents typically include physicians, such as anesthesiologists, with privileges at the hospital. It is

important to note that physicians have a professional duty of confidentiality towards patients irrespective of their role as HIC or agent. Indeed, anesthesiologists have a duty to keep PHI confidential and secure, and only collect, use, or disclose PHI for the purpose of providing care or for other authorized purposes.[6] Other authorized purposes include the collection, use, or disclosure of PHI to comply with a court order or when the disclosure is expressly authorized or required by legislation (e.g., mandatory reporting obligations regarding children in need of protection, or concerns about a patient's fitness to drive, etc.).

While HICs have custody of the PHI stored in EMR, the PHI is essentially held in trust for patients. This requires that a patient's consent should generally be obtained to collect, use, and disclose their PHI.[6–8] Nevertheless, as is discussed further, a patient's expressed consent is not required in certain situations, which are generally outlined in the applicable statute.

Access to EMR based on implied patient consent

Individuals who need to know a patient's PHI for the purpose of providing healthcare to that patient form the patient's "circle of care".[9] Individuals within that circle can include physicians, nurses, pharmacists, clinical clerks, medical students, etc.[8,10] The term "circle of care" is not explicitly defined in privacy statutes. Nevertheless, it can be useful to conceptualize how PHI can be collected, used, and disclosed without the patient's express consent.

Individuals within the circle of care can generally rely on a patient's implied consent to view, use, and share the patient's PHI with one another. In some provinces, to rely on the patient's implied consent, the PHI must have been received from the patient to whom the PHI relates (or a substitute decision-maker) or from another HIC or agent. The PHI must have been received for the purpose of providing healthcare to that patient and must be used or disclosed by a HIC or agent for that same purpose.[6,11]

Let us imagine a situation where everyone who works at a hospital has access to PHI stored in a shared EMR system. Is having such access sufficient to allow anyone to view a patient's PHI based on the patient's implied consent? No. Only those who need to view the patient's PHI in order to provide healthcare to that patient can generally access the EMR to view that information based on implied consent.

Similarly, if an anesthesiologist was involved in a high-profile patient's care, for example, and wants to view that patient's PHI purely out of curiosity or personal interest, for purposes unrelated to ongoing medical care, he or she cannot access the EMR on the basis of implied consent. Nevertheless, if the purpose of viewing the PHI is to provide ongoing care, the anesthesiologist would be within the circle of care and could rely on the patient's implied consent to access the EMR.

Even within the circle of care, patients can impose limits on who can collect, use, or disclose their PHI. These restrictions are sometimes referred to as "lock-box requests" and take the form of directives from a patient that his or her entire record, or certain information in the record, may only be accessed (or must not be accessed) by specified individuals or groups of individuals.[5] Healthcare providers cannot rely on the patient's implied consent if they are aware that the patient has imposed such limits.[11]

Access to EMR based on authorized secondary uses of PHI

Recognizing the value of PHI for purposes other than providing healthcare, privacy statutes authorize healthcare providers to access EMRs and use PHI for certain secondary purposes without having to obtain the patient's express consent.[2] Authorized secondary uses of PHI vary from one privacy statute to the next. For example, HICs may be authorized, and may authorize their agents, to use PHI without the patient's consent to manage internal operations, provide staff education, perform internal investigations, undertake practice reviews to improve quality of care, and conduct approved health research.[2,5,12]

Physicians working in an institution should be careful not to access the institution's EMR and use PHI for a secondary purpose unless they have knowledge of the regulatory framework in their jurisdiction and authority from the institution. The use of PHI for a secondary purpose is often part of an institutional initiative and may require explicit permission. For instance, a hospital may have a policy requiring the Chief of Department's permission before using PHI for quality of care audits or for sharing PHI as part of staff education. Anesthesiologists should inquire with their hospital administration about relevant internal policies or directives.

Similarly, data from an EMR should not be used in research without consideration of the regulations and policies that apply in their jurisdiction and institution. Privacy legislation in some provinces requires that research using PHI without the consent of the individual be approved by a research ethics board. These boards will consider a variety of factors such as whether the research can be conducted without using identifiable information, the safeguards that are in place to protect the information, whether the research is in the public interest, and whether obtaining consent from the research subjects would be impractical. Often, research ethics boards may not approve the use of personal health information in clinical trials

without the consent of the individual.[13] These factors apply equally when the PHI is kept in EMR.

Conclusion

Given the legal complexities related to PHI, anesthesiologists are understandably wary about privacy risks when accessing EMR. As discussed, healthcare providers should generally only access EMR to view the limited PHI that they need to know for providing healthcare to a patient. Likewise, PHI should only be used for providing healthcare to the patient and shared within the circle of care, unless it is otherwise authorized by statute or the patient's express consent.

When implementing an EMR system, policies should be put in place to ensure that PHI is collected, used, and disclosed for authorized purposes.[6,8] The HICs and their agents should also understand their obligations in the event of a privacy breach. For example, privacy statutes in a number of provinces require HICs to send a notice of the privacy breach to affected individuals and/or the privacy commissioner.[14]

Given that privacy obligations vary across Canada, it is important for anesthesiologists and other physicians to be familiar with the specific requirements applicable where they practice.

Bien comprendre les risques d'atteinte à la vie privée lors de l'accès aux dossiers médicaux informatisés

Le secteur des soins de santé canadien assiste à une augmentation de l'utilisation des technologies pour gérer les renseignements personnels sur la santé (RPS); en effet, la majorité des fournisseurs de soins de santé substituent aujourd'hui leurs dossiers papier pour des dossiers médicaux informatisés (DMI).[1]

Les soins de santé modernes nécessitent une collaboration et une coordination interprofessionnelles. Ces composantes sont particulièrement importantes dans un contexte hospitalier, où un patient reçoit souvent des soins de plusieurs intervenants, notamment des urgentologues, chirurgiens, anesthésiologistes et infirmières. Les systèmes de dossier médical informatisé facilitent la fourniture de soins de santé modernes car ils permettent à d'importants volumes de RPS d'être entreposés et partagés.[2]

Alors que les DMI offrent des avantages considérables, notamment un échange d'informations facilité afin de prodiguer des soins de qualité au moment opportun, ces dossiers posent également des risques inhérents d'atteinte à la vie privée. Les mêmes exigences générales de confidentialité s'appliquent aux dossiers médicaux papier et informatisés, mais la possibilité d'accéder à un DMI par un grand nombre d'utilisateurs et l'accès potentiel depuis plusieurs lieux sont deux exemples très concrets des nouveaux défis de gestion du risque posés par cette méthode améliorée de tenue de dossiers. Ces risques ont été mis en lumière dans de nombreux cas, dans lesquels des cas de violation de la vie privée sont survenus en raison d'accès non autorisés aux DMI afin de consulter, d'utiliser ou de divulguer des RPS.[3,4] Bien que l'accès non autorisé puisse être motivé par des intérêts financiers ou personnels, il pourrait également être le fruit d'un malentendu de bonne foi quant aux obligations de chacun en matière de confidentialité.

Au Canada, la collecte, l'utilisation et la divulgation des RPS sont gouvernées par un amalgame de législations fédérales, provinciales et territoriales.[5] Les organismes de règlementation médicaux (c.-à-d. les 'collèges' provinciaux) disposent également de nombreux règlements, politiques et règles. En raison de l'évolution des cadres législatifs et règlementaires, les obligations quant à la protection de la vie privée peuvent être difficiles à naviguer. Ces cadres varient également d'une province à l'autre, c'est pourquoi il est essentiel que les médecins comprennent les exigences spécifiques applicables à la juridiction dans laquelle ils pratiquent.

L'Association canadienne de protection médicale reçoit régulièrement des appels de médecins à la recherche de conseils médicolégaux ou d'aide en ce qui touche aux DMI et aux questions de protection de la vie privée. Cet article propose quelques réflexions générales dans l'optique de clarifier les obligations en matière de confidentialité dans un tel contexte, notamment en ce qui touche aux personnes autorisées à avoir accès aux DMI pour consulter, utiliser ou divulguer des RPS, et à quelles fins.[A]

L'accès aux DMI à des fins de consultation, d'utilisation ou de divulgation de RPS

Le rôle des dépositaires de renseignements sur la santé

Un dépositaire de renseignements sur la santé (DRS)[B] est une entité qui a le contrôle sur les RPS qui se trouvent sous sa garde. Les administrateurs d'hôpitaux et les propriétaires de cliniques constituent des exemples typiques de DRS pour les RPS enregistrés dans leurs établissements.[C] Ces DRS sont responsables de la récolte, de l'utilisation et de la

divulgation des RPS conformément au cadre législatif et règlementaire applicable. Cela comprend la prise de mesures afin d'éviter tout accès, utilisation ou divulgation non autorisé de RPS.[6]

Les DRS peuvent désigner des agents[D] qui agiront en leur nom et rempliront leurs obligations de confidentialité.[6] Lorsque l'hôpital est le DRS, les agents sont traditionnellement des médecins tels que des anesthésiologistes possédant des privilèges à l'hôpital. Il est important de souligner que les médecins ont une obligation professionnelle de confidentialité envers les patients indépendamment de leur rôle en tant que DRS ou agent. En effet, les anesthésiologistes ont l'obligation de garder les RPS confidentiels et en sécurité et de ne récolter, utiliser ou divulguer les RPS qu'aux fins de prodiguer des soins ou à d'autres fins autorisées.[6] Parmi les autres fins autorisées, citons la collecte, l'utilisation ou la divulgation des RPS afin de respecter une ordonnance ou lorsque la divulgation est expressément autorisée ou requise par la loi (par ex. obligations de communication concernant les enfants devant être protégés, ou inquiétudes quant à la capacité de conduire d'un patient, etc.).

Bien que les dépositaires de renseignements de santé aient la garde des RPS enregistrés dans les DMI, les RPS sont principalement tenus en fiducie pour les patients. En d'autres termes, le consentement d'un patient devrait généralement être obtenu pour récolter, utiliser et divulguer ses RPS.[6–8] Toutefois, comme nous l'expliquerons plus loin, le consentement exprès d'un patient n'est pas requis dans certaines situations, lesquelles sont généralement décrites dans la loi applicable.

L'accès aux DMI fondé sur le consentement implicite du patient

Les personnes qui ont besoin d'avoir accès aux RPS d'un patient afin de lui prodiguer des soins de santé forment ce qu'on appelle le « cercle de soins » d'un patient.[9] Les personnes dans ce cercle peuvent être des médecins, des infirmières, des externes, des étudiants en médecine, etc.[8,10] Le terme « cercle de soins » n'est pas explicitement défini dans les lois sur la protection de la vie privée. Il peut cependant s'avérer utile pour conceptualiser la façon dont les RPS peuvent être récoltés, utilisés et divulgués sans le consentement exprès du patient.

Les personnes qui font partie du cercle de soins peuvent en général se fier au consentement implicite d'un patient pour consulter, utiliser et partager entre elles les RPS du patient. Dans certaines provinces, pour prendre pour acquis le consentement implicite du patient, les RPS doivent avoir été obtenus du patient auquel les RPS s'appliquent (ou d'une personne déléguée) ou d'un autre DRS ou agent. Les RPS doivent avoir été reçus aux fins de fourniture de soins de santé à ce patient et doivent être utilisés ou divulgués par un DRS ou un agent aux mêmes fins.[6,11]

Imaginons une situation dans laquelle toutes les personnes travaillant dans un hôpital ont accès aux RPS enregistrés dans un système partagé de DMI. Suffit-il d'avoir un tel accès pour permettre à quiconque de consulter les RPS d'un patient en s'appuyant sur le consentement implicite d'un patient? La réponse est non. Seules les personnes qui ont besoin de consulter les RPS d'un patient afin de lui prodiguer des soins peuvent en général avoir accès à son DMI afin de consulter ces informations et ce, sur la base d'un consentement implicite.

De la même manière, si un anesthésiologiste participait aux soins d'un patient célèbre, par exemple, et qu'il souhaitait consulter les RPS du patient par pure curiosité ou par intérêt personnel, à des fins sans rapport avec les soins médicaux en cours, il ne pourrait pas avoir accès au DMI sur la base d'un consentement implicite. En revanche, si l'objectif de consultation des RPS était de prodiguer des soins en cours, alors l'anesthésiologiste serait dans le cercle de soins et pourrait donc prendre pour acquis le consentement implicite du patient afin d'avoir accès à son DMI.

Même au sein du cercle de soins, les patients sont en droit d'imposer des limites quant aux personnes autorisées à récolter, utiliser ou divulguer leurs RPS. On parle parfois de « demande de verrouillage »; ces demandes peuvent prendre la forme de directives d'un patient selon lesquelles son dossier en entier, ou certains renseignements de son dossier, ne peut être consulté que (ou ne doit pas être consulté) par certaines personnes ou certains groupes de personnes en particulier.[5] Les fournisseurs de soins de santé ne peuvent pas prendre pour acquis le consentement implicite d'un patient s'ils savent que leur patient a imposé de telles limites.[11]

L'accès aux DMI fondé sur les utilisations secondaires autorisées des RPS

Reconnaissant la valeur des RPS pour d'autres fins que pour la fourniture de soins de santé, les lois sur le respect de la vie privée autorisent les fournisseurs de soins à avoir accès aux DMI et à utiliser les RPS pour certains objectifs secondaires sans avoir à obtenir le consentement exprès du patient.[2] Les utilisations secondaires autorisées des RPS varient d'une loi sur la vie privée à l'autre. Par exemple, un DRS pourrait être autorisé, et autoriser ses agents, à utiliser des RPS sans le consentement du patient afin de gérer les opérations internes, de former le personnel, de réaliser des enquêtes internes, d'entreprendre des revues de la pratique

afin d'améliorer la qualité des soins, et de mener des recherches en santé approuvées.[2,5,12]

Les médecins travaillant dans un établissement ne devraient accéder aux DMI de cet établissement et utiliser les RPS à des fins secondaires que s'ils connaissent le cadre règlementaire spécifique à leur lieu de travail et qu'ils ont les permissions nécessaires de leur établissement. L'utilisation de RPS pour un objectif secondaire se fait souvent dans le cadre d'une initiative de l'établissement et pourrait nécessiter une permission explicite. Par exemple, un hôpital pourrait disposer d'une politique exigeant la permission du chef de département avant d'utiliser des RPS pour un contrôle de la qualité des soins ou de partager des RPS dans le cadre de formation du personnel. Les anesthésiologistes devraient se renseigner auprès de l'administration de leur hôpital concernant les politiques ou directives internes pertinentes.

De la même manière, les données d'un DMI ne devraient pas être utilisées en recherche sans tenir compte des règles et politiques applicables dans leur juridiction et établissement. Dans certaines provinces, les lois sur la vie privée exigent que toute recherche utilisant des RPS sans le consentement de la personne soit approuvée par un comité d'éthique de la recherche. Ces comités tiendront compte de divers facteurs, en déterminant si la recherche peut être réalisée sans utiliser d'informations nominales, en identifiant les garanties en place pour protéger les renseignements, en évaluant si la recherche est d'intérêt public et si l'obtention du consentement serait irréalisable, entre autres. Bien souvent, les comités d'éthique de la recherche pourraient ne pas approuver l'utilisation de renseignements personnels sur la santé dans les études cliniques sans obtenir le consentement individuel.[13] Ces facteurs s'appliquent également lorsque les RPS sont enregistrés dans des DMI.

Conclusion

Étant donné les complexités légales liées aux RPS, les anesthésiologistes sont, avec raison, prudents quant aux risques de bris de la confidentialité lorsqu'ils consultent des DMI. Comme nous l'avons démontré, les fournisseurs de soins de santé ne devraient, en règle générale, avoir accès aux DMI que pour consulter les RPS qui pourraient être nécessaires à la provision de soins de santé à un patient. De la même manière, les RPS ne devraient être utilisés que pour fournir des soins de santé au patient et partagés exclusivement avec le cercle de soins, à moins que la loi n'autorise leur accès ou que le patient ait donné son consentement exprès.

Lors de la mise en œuvre d'un système de DMI, des politiques devraient être mises en place pour garantir que les RPS soient récoltés, utilisés et divulgués à des fins autorisées.[6,8] Les DRS et leurs agents devraient également comprendre leurs obligations en cas de bris de confidentialité. Par exemple, les lois sur la vie privée de plusieurs provinces exigent du DRS qu'il fasse parvenir un avis de bris de confidentialité aux personnes touchées et/ou au commissaire à la protection de la vie privée.[14]

Étant donné que les obligations en matière de respect de la vie privée varient au sein même du Canada, il est important que les anesthésiologistes et autres médecins connaissent les exigences spécifiques à leur lieu de pratique.

Footnotes

A. This article is not intended to provide legal advice.

B. Health information custodians are also known as "trustees" under certain privacy legislation.

C. In some provinces, physicians working in a clinic will continue to be considered the HIC.

D. Agents are also known as "affiliates" under certain privacy legislation.

Funding statement None.

Conflicts of interest None.

Editorial responsibility This submission was handled by Dr. Hilary P. Grocott, Editor-in-Chief, *Canadian Journal of Anesthesia.*

Conflit d'intérêt Aucun.

Déclaration de financement Aucune.

Responsabilité éditoriale Cet article a été traité par Dr Hilary P. Grocott, rédacteur en chef, *Journal canadien d'anesthésie*.

References

1. *Canada Health Infoway*. Year in review 2017–2018. Highlights from 2017 to 2018: 85% of primary care physicians in Canada reported using an EMR in 2017. Available from URL: https://www.infoway-inforoute.ca/en/component/edocman/3556-annual-report-2017-2018/download?Itemid=0 (accessed October 2019).
2. *Cavoukian A, Alvarez RC*. Embedding privacy into the design of EHRs to Enable Multiple Functionalities – Win/Win. Electronic Healthcare Law Review, Vol 1, No. 4 (June 2012). Also Available from URL: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-ehr-e_1.pdf (accessed October 2019).
3. *Court of Appeal for Ontario*. Hopkins v Kay, 2015 ONCA 112. Available from URL: https://www.canlii.org/en/on/onca/doc/2015/2015onca112/2015onca112.pdf (accessed October 2019);
4. *Office of the Saskatchewan Information and Privacy Commissioner*. Investigation Report 177-2018 (inappropriate

access of PHI of patients injured in Humboldt Broncos bus crash by physicians not directly involved in the patients' care); Available from URL: https://oipc.sk.ca/assets/hipa-investigation-177-2018.pdf (accessed October 2019).
5. *Nelson E*, *Ogbogu U*. Law for Healthcare Providers. Toronto: LexisNexis; 2018 .
6. *Canadian Medical Protective Association*. Electronic Records Handbook; 2014. Available from URL: https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/handbooks/com_electronic_records_handbook-e.pdf (accessed October 2019).
7. *Canadian Medical Protective Association*. Releasing a patient's personal health information: What are the obligations of the physician? (October 2012). Available from URL https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2012/releasing-a-patient-s-personal-health-information-what-are-the-obligations-of-the-physician (accessed October 2019).
8. *Inions NJ*, *Tran LE*, *Rozovsky LE*. Canadian Health Information: A Practical Legal and Risk Management Guide. 4th ed. Toronto: LexisNexis; 2018 .
9. *Saskatchewan Information and Privacy Commissioner*. IPC Guide to HIPA. The Health Information Protection Act. December 2016: 35-6. Available from URL: https://oipc.sk.ca/assets/ipc-guide-to-hipa.pdf (accessed October 2019).
10. *Erdman J*, *Gruben V*, *Nelson E*. Canadian Health Law and Policy. 5th ed. Toronto: LexisNexis; 2017 .
11. *Information and Privacy Commissioner of Ontario*. Circle of Care Sharing Personal Health Information for Health-Care Purposes (August 2015). Available from URL: https://www.ipc.on.ca/wp-content/uploads/resources/circle-of-care.pdf (accessed October 2019).
12. For example, in Ontario see Personal Health Information Protection Act, 2004, SO 2004, c 3, Sched 4, s 37.
13. *Canadian Medical Protective Association*. Physicians and research: Understanding the legal, ethical, and professional obligations (July 2014). Available from URL: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2014/physicians-and-research-understanding-the-legal-ethical-and-professional-obligations (accessed October 2019).
14. *Ceresia PJ, et al*. Privacy and Healthcare Providers: Moving Beyond the Duty of Confidentiality, Electronic Healthcare Law Review, Vol 1 No. 2 (December 2011).