SAFEGUARD

A QUARTERLY NEWSLETTER PUBLISHED BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 02, ISSUE 01 FEBRUARY 2018

CONTACT INFORMATION

Office of the Information and Privacy Commissioner
3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
E-mail: commissioner@oipc.nl.ca
www.oipc.nl.ca

"Thus, at least in part, medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient."

- Justice La Forest
McInerney v. MacDonald, [1992] 2 SCR 138 (SCC)

- OIPC Reminders and Updates
- Who is Responsible for Privacy?
- Use of Email to Send Personal Health Information
- APSIM 2018 Reminder
- Privacy vs. Confidentiality
- Interesting News & Decisions

OIPC REMINDERS AND UPDATES

Privacy Management Program framework

The OIPC has created a Privacy Management Program framework designed to provide step-by-step guidance on how custodians can implement effective and accountable privacy management programs. A privacy management program ensures that privacy is built into all initiatives, programs or services. The framework will soon be accessible on our website.

PRACTICE TIP

Custodians should limit knowledge of the identity of access applicants to only those who need the information to process the request. By limiting the number of individuals who know the applicant's identity, requests can be processed in a fair, open, accurate and complete manner.

The following tips will assist in maintaining an applicant's anonymity:

1. Always refer to an applicant as "the applicant" or by an assigned request number.
2. If a request is made by an employee, documents associated with the request should not be placed on the employee's personnel file.
3. Restrict access to paper and electronic documents that deal with processing the request.
4. Develop and implement a policy regarding preserving the anonymity of access applicants.

WHO IS RESPONSIBLE FOR PRIVACY?

Privacy, and the larger subject of information protection, is everyone's responsibility. So what can you do to change perceptions and promote collaboration?

Get Support from the Top

Under *PHIA*, custodians are accountable for ensuring personal health information ("PHI") is protected, among other requirements. While custodians may designate a person to be responsible for the day-to-day management of this task, the custodian remains accountable. Where a custodian is not an individual, the custodian should ensure that the custodian's executive is aware of privacy obligations and that the entire management team demonstrates support for privacy initiatives publically and within the organization.

Resource Adequately

Individuals with delegated responsibilities for privacy require a variety of resources. First and foremost, they need training in privacy, including legislation and available tools. They also need to be able to dedicate adequate time to privacy. While some time will be spent on privacy complaints and breach reports, time should also be devoted to proactive initiatives, such as developing a privacy management program and writing privacy impact assessments (PIAs).

Build an Inner Circle

Everyone has a role to play. Managers and directors, especially those overseeing programs and staff that collect, use and disclose PHI, are responsible for ensuring appropriate policies and procedures are in place and their staff are aware of privacy expectations. Individuals responsible for privacy should also have close ties with professionals involved in information management, information technology, security, risk management, human resources and policy.

Develop a Privacy Education Program

Custodians must offer training and awareness activities to educate all staff and contractors on privacy obligations and affiliated policies and procedures. These programs should also promote the role everyone plays in protecting PHI such that all staff are aware of their responsibilities. Use training and awareness activities to ensure everyone understands their own role in protecting PHI. Remind them that the information they are protecting, in many cases, includes their own PHI and/or that of family, neighbours and friends.

Collaborate

Privacy requires collaboration. It takes an entire organization, from the bottom to the top, to ensure that PHI is protected. If anyone in your organization can cause a breach, then everyone has a role to play in protecting PHI. When everyone works together to protect PHI, everyone benefits.

USE OF EMAIL TO SEND PERSONAL HEALTH INFORMATION

Section 15 of *PHIA* requires that a custodian take reasonable steps to ensure that the PHI in its custody or control is protected against theft; loss; unauthorized access, use or disclosure; and unauthorized copying or modification. The section also mandates that records containing PHI be retained, transferred and disposed of in a secure manner.

The communication of PHI may only be carried out in accordance with the collection, use and disclosure provisions of *PHIA*. Inherent risks associated with email should be addressed before using it as a method of communicating PHI to clients or their substitute decision-makers. Custodians need to be aware that their email records, as with any other format, could be subject to an investigation by the Commissioner if there is a complaint relating to any aspect of *PHIA.*

Below are practices and tools custodians can utilize when communicating PHI via email:

Prior to Sending PHI in an Email

- Conduct a Privacy Impact Assessment of the practice.
- Create written policies and procedures, in accordance with section 13 of *PHIA*, surrounding sending and receiving PHI via email.
- Provide and require ongoing privacy and security training.
- Consider whether email is the best way to communicate the information and whether another, more secure method is available.

Sending an Email Containing PHI

- Limit the amount of PHI being sent to only what is necessary. Ensure that no PHI is in the subject line of the email.
- Only place essential information in the body of the email.
- Send PHI as an encrypted, locked attachment. Communicate the password using a separate method.
- Use a professional, as opposed to personal, web-based email account to send the email.
- Verify the email address with the intended recipient(s) and re-check the email addresses, cc and bcc fields and attachments before sending.
- Turn off autocomplete or autofill options.
- Use read/received/delivery receipts where possible.
- Add a disclaimer to your signature regarding misdirected emails and their destruction.
- Maintain copies in the client file.

For further discussion, see our full Guidance Document.

APSIM 2018 REMINDER

The APSIM conference is scheduled for April 30th to May 2nd, 2018 at Memorial's School of Medicine. This FREE conference is designed to bring together professionals from Access, Privacy, Security and Information Management to promote collaboration and build awareness of the overlap and interplay in the groups' roles so that we may assist each other in the management, protection, and security of information. Registration will open soon.

PRIVACY VS. CONFIDENTIALITY

Privacy and confidentiality are often mistakenly used interchangeably. It is not uncommon for individuals who inappropriately access PHI to hold the belief that they have not breached someone's privacy because they have not disseminated the information which they accessed. This belief is incorrect.

Privacy is the right of an individual to have their PHI protected from inappropriate actions as per *PHIA*. Confidentiality relates to the limitations on disseminating information.

Inappropriate access to PHI is a breach of privacy.

Inappropriate disclosure of PHI is a breach of privacy and confidentiality.

When it comes to PHI, breaches of privacy will not always include a breach of confidentiality; however, a breach of confidentiality will always amount to a breach of privacy.

Privacy rights and obligations are codified in legislation such as *PHIA*. Confidentiality obligations generally stem from internal policies and procedures, including oaths/affirmations of confidentiality. It is incumbent upon a custodian to educate and train its staff on the distinction between these two concepts. Custodians and their staff need to be aware of when they are entitled to access PHI and the limitations on disclosure of that information.

For more discussion on this topic, see the Office of the Saskatchewan Information and Privacy Commissioner's blog "Privacy vs. Confidentiality".

INTERESTING NEWS & DECISIONS

Alleged Inappropriate Alterations to Medical Records

Investigators for the College of Physicians and Surgeons of Saskatchewan found a Regina doctor altered the medical records of a woman who died hours after being in her care. The College found that there were multiple alterations over the course of 8 months and were so prevalent that the patient's record was no longer an accurate reflection of the care interaction.

Office of the Saskatchewan Information and Privacy Commissioner IR 300-2017

The Trustee proactively reported a privacy breach to the Saskatchewan IPC when it discovered that personal health information from a 16-day period was lost or not recorded to its electronic medical record. The Trustee's EMR is hosted on a server located within its premises. The Trustee indicated data is saved onto the local server and then backed up locally within its own office and remotely offsite with its IT service provider. Following the loss, the Trustee was informed by its IT service provider that all data for a 16-day period was lost. Data was not saved to the server nor was it being backed up locally or remotely.

The IPC found that the Trustee had made reasonable efforts to address the privacy breach and is now taking appropriate steps to prevent or minimize the likelihood of a similar privacy breach in the future.