RISK REFERENCE SHEET

Privacy Breach

All sectors

Patients expect that their personal health information (PHI) will be collected, used and disclosed by healthcare providers for the purposes of providing health care and/or health services. Healthcare organizations have a duty to ensure that PHI in their custody is protected against unauthorized use, disclosure, electronic transfer, copying, modification, disposal, theft or loss. Negative consequences arising from a breach in privacy can be far-reaching and include lawsuits, reputational damage, and cyber-attacks. The loss and theft of mobile devices (e.g. laptop computers, external hard drives, flash drives and USB keys) have the potential to lead to breaches involving hundreds/thousands of patients, which could result in class action lawsuits. More recently, healthcare organizations have faced class actions as a result of employees snooping into records of PHI or selling PHI to third parties for a profit. While the privacy law is rapidly evolving and differs from one province to another, patients whose PHI has been breached may seek compensation. In addition, staff who breach patient privacy may face serious consequences, including termination, discipline by their professional college, and possibly criminal charges.

COMMON CLAIM THEMES

- Lack of response to a patient's expressed request to restrict access to their PHI.
- Insufficient technological safeguards to:
  - Restrict unauthorized access to electronic records;
  - Regularly and efficiently audit staff access.
- Lack of encryption and storage controls on mass storage devices (e.g. laptops and USB keys).
- Computer systems without set security profiles or audit functions.
- Staff member snooping into health records of a family member, friend, celebrity or person with whom he or she has a personal conflict.
- Staff member accessing patient health records to sell PHI for financial gain.
- Failure to notify the insurer in a timely manner, and notification of patients before completing a thorough investigation to determine the extent and scope of the breach.
- Lack of compliance with privacy policies and procedures.

CASE STUDY 1

A patient made a written request to the healthcare organizations' privacy officer to ensure their health record remained private. The patient subsequently became aware that their estranged spouse, a healthcare provider at the healthcare organization had accessed their health record. The estranged spouse's new partner had also viewed the patient's health record on a number of occasions. The patient brought the incident to the attention of the healthcare organization's privacy officer and the provincial privacy commission. The Office of the Privacy Commissioner issued an order against the healthcare organization with respect to a number of violations related to the handling of the case.

CASE STUDY 2

A healthcare organization's employee breached confidentiality by accessing the health records of a patient hundreds of times. The employee accessed files from the healthcare organization where they worked as well as from another healthcare organization through a shared health records application. The employee used the PHI to harass the patient and disclosed the patient's PHI to the patient's family, friends, and employer. The employee was terminated. The patient sued the healthcare organization and the employee. The healthcare organization was found not to be at fault, but the employee was required to pay the patient an out-of-pocket settlement.

Canadian Case Examples

Privacy Breach

REFERENCES

- HIROC claims files.
- Cavoukian, A., & El Emam, K. (2011, June). Dispelling the myths surrounding de-identification: Anonymization remains a strong tool for protecting privacy. Toronto, ON: Information and Privacy Commissioner of Ontario.
- DeSouza, P. (2010, Fall). Protecting personal health information. *The HIROC Connection, 26*, 1-2.
- HIROC. (2015, April). Critical incidents and multi-patient events risk resource guide.
- Information and Privacy Commissioner of Ontario. (n.d.). What to do when faced with a privacy breach: Guidelines for the health sector.
- Information and Privacy Commissioner of Ontario. (2011, February). Applying PHIPA and FIPPA to personal health information: Guidance for hospitals.
- Information and Privacy Commissioner of Ontario. (2012, December). Encryption by default and circles of trust: Strategies to secure personal information in high-availability environments.
- Information and Privacy Commissioner of Ontario. (2015, January). Detecting and deterring unauthorized access to personal health information.
- Office of the Privacy Commissioner of Canada. (n.d.). Key steps for organizations in responding to privacy breaches.
- Office of the Saskatchewan Information and Privacy Commissioner. (2015, July). Privacy breach guidelines.
- Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Schedule A.

Date last reviewed: March 2016

RISK REFERENCE SHEET

Privacy Breach

MITIGATION STRATEGIES

Note: The Mitigation Strategies are general risk management strategies, not a mandatory checklist. Refer to the HIROC Critical Incidents & Multi-Patient Events Risk Resource Guide for more information on managing multi-patient events.

Reliable Prevention Processes

- ☐ Adopt a policy outlining appropriate collection, storage, use, transfer disclosure and destruction of patient records and sensitive administrative documents.
- ☐ Ensure processes allowing patients to restrict access to their PHI.
- ☐ Ensure appropriate authentication processes for staff accessing systems on which PHI is maintained (including but not limited to approvals for system access, the use of strong passwords, non-sharing of passwords and scheduled prompts to change passwords.
- ☐ Prohibit the removal of identifiable PHI in any form (i.e. paper or electronic) from the healthcare organization, unless required for the provision of medical care.
- ☐ Prohibit: the storage of identifiable PHI on mobile devices; ensure data encryption of laptops; USB keys; tablets; smart phones; and enable secure remote access and/or virtual private networks as an alternative to removing PHI.
- ☐ Ensure that stored records used for research are de-identified and/or coded, and that the code needed to unlock identities is stored separately on a secure computer or server.
- ☐ Ensure there are written contractual agreements with any agent retained to store or dispose of paper PHI records, stipulating that no unauthorized persons will have access to the records from the time they leave the custody of the healthcare organization to their storage or destruction locations, and that destruction entails irreversible shredding or pulverization.
- ☐ Ensure the protection of physical records after hours with at least two levels of security (e.g. two locked doors or a locked door and locked filing cabinet).

Education

- ☐ Ensure staff, volunteers, physicians and researchers are trained in their duties and obligations related to the collection, protection, use and disclosure of PHI, including data management, strict prohibition on sharing user IDs and passwords, the risks of using mobile devices, taking photographs and the consequences for those that disregard their duties.

Breach Management and Look Backs

- ☐ Develop a privacy breach protocol which ensures immediate internal notification of actual or potential breaches and steps to prevent further unauthorized use or disclosure.
- ☐ Establish a protocol/checklist/algorithm for the management of multi-patient/significant breaches, including timely investigation, documentation, patient and insurer notification (please see below for additional information), and that the facility's chief privacy officer, risk management and legal experts are consulted to determine the appropriate threshold for disclosure and (along with communications professionals) to determine the appropriate process for carrying this out.
- ☐ Notify HIROC before any investigation is commenced as per the HIROC policy. Financial coverage will be available for independent legal and required specialties for investigation based on experts' determination of disclosure requirements and HIROC's determination the adequacy of notification by the insured.
- ☐ Ensure all records and information related to look backs (including details of the information breaches) are maintained and retained.
- ☐ Ensure the timely notification of the provincial/ territorial information and privacy office where warranted.
- ☐ Take appropriate disciplinary action with individuals who are found to have violated known duties and obligations related to the protection, use and disclosure of PHI.

Monitoring and Measurement

- ☐ Monitor implementation of recommendations resulting from investigations of privacy breaches to mitigate the risk of recurrence.
- ☐ Ensure clinical software applications have audit functionality.
- ☐ Implement formal strategies to help ensure consistent adherence to privacy policies/practices (e.g. periodic chart/e-record audits, analysis of reported incidents/ events, learning from medico-legal matters).