RISKCHECK
BY MARSH CANADA LTD.

Fall 2023

Physical Protection of Patient Records

Healthcare entities have the ethical, professional, and legal obligations to protect patient records under its custody; they must adopt the appropriate safeguards to ensure that the paper and electronic files are adequately protected. Specifically, safeguards refers to any controls that protect patient files and record, including physical measures that should be proportionate to the degree of sensitivity of information contained in the patient records.

As part of their approach to protecting patient records, healthcare entities will need to consider its range of risks and address them through a layer of controls as part of a comprehensive risk management plan. In doing so, they will be able to strengthen their policies, procedure, and practices with a targeted focus on access, storage, and usage of patient records.

The following guidance highlights key areas of considerations for healthcare entities in protecting patient records under their custody. It should not be seen as an exhaustive list and should be used in conjunction with internal policies and procedures, as well in compliance with local laws and regulations, as some of the recommendations made in this document may be legally required.

1. Policies and Procedures

Establishing a policy and procedure is essential in providing guidance to adopting safeguards protect patient records. Specifically, it should clearly convey the position of the entity while providing guidance on specific safeguards to adopt related to the access, storage, and usage of patient records under its custody.

- ☐ Develop a comprehensive policy and procedure that addresses:
  - ☐ Physical protection of patient records, including during access, storage, and usage; and
  - ☐ Use of appropriate physical protection appropriate to the sensitivity of file and information.
- ☐ Each of the above policies and procedure should include but not limited to the following:
  - ☐ Commitment to safeguarding patient records under its custody;
  - ☐ Establishment of where the policy and procedures are enforced;
  - ☐ Articulates accountability of all parties:
    - ☐ Employees;
    - ☐ Independent practioners (e.g. physicians, midwives);
    - ☐ Volunteers;
    - ☐ Students;
    - ☐ Vendors; and
    - ☐ Patients/Families.
  - ☐ Articulates unacceptable behaviour;
  - ☐ Available support services internal and external to the organization;

- ☐ Clearly defines and provides examples of patient records:
  - ☐ Physician order and progress notes;
  - ☐ Nursing and allied health progress notes;
  - ☐ Health history and assesmsent notes;
  - ☐ Medical history and administration notes;
  - ☐ Diagnostic imaging results and notes; and
  - ☐ Laboratory results and notes.
- ☐ Clearly defines and provides examples of physical controls and access measures
  - ☐ Locked file cabinets, desks, closets;
  - ☐ Restricted office spaces;
  - ☐ Mechanical locks and access (e.g. keys); and
  - ☐ Electronic locks and access (e.g. ID badge, card swipe, keypad).
- ☐ Ensure that training regarding the policy is provided to all indivduals and groups, as required; and
- ☐ Ensure the policy is made available to all individuals and goups, as required.

2. Access

Healthcare entities need to consider the types of patient records under its custody and adopt the appropriate physical measures to safeguard all files and records. As an initial step, healthcare entities will need to address physical access throughout their premises. The physical access and security measures that should be adopted by healthcare entities should include the following:

- ☐ Establish physical access control for designated areas through a blend of the following controls:
  - ☐ Mechanical access (e.g. keys);
  - ☐ Electronic access swipes (e.g. fobs, badges, keypads);
  - ☐ Alarm keypad systems (mechanical or electronic); and
  - ☐ Change keypad access codes on a regular basis.
- ☐ Install alarm systems to monitor authorized and unauthorized access to designated areas;
- ☐ Change alarm system passcodes on a regular basis; and
- ☐ Appoint designated individual(s) to manage and document access management.

3. Storage

As healthcare entities take steps to safeguard patient records under their custody, a secondary consideration includes the physical storage of patient records. As an added area of consideration, healthcare entities can adopt a combination of measures as they transition from paper-based files and records to electronic medical records. The security measures that should be adopted by healthcare entities should include the following:

- ☐ Patient records must be physically stored with any of the following:
  - ☐ Lockable file drawers or cabinets;
  - ☐ Controlled access room/area; and
  - ☐ Controlled access building.
- ☐ Patient records in a non-controlled access area must be:
  - ☐ Stored in a lockable file drawers or cabinets;
  - ☐ Placed in a location where unauthorized individuals cannot view the files or records;
  - ☐ Not left unattended at printers, photocopiers, and fax machines; and
  - ☐ Returned to the secured filing location (e.g. lockable drawer/cabinet) as soon as possible.

4. On-Premise Use

As patient records are accessed and used during the delivery of healthcare services, healthcare entities need to ensure that authorized individuals take the necessary measures to prevent any unauthorized access or use. In addition to the physical measures related to access and storage, the following security measures should be adopted to strengthen practices at point of care:

- ☐ Close the drawers and cabinets when not in active use;
- ☐ Lock the drawers and cabinets when leaving the area or workstation;
- ☐ Position screens or displays that contain patient information away from plain view; and
- ☐ Cover any files or records that contain patient information when in use but not actively being viewed.

5. Off-Premise Use

As there are instances where patient records are required to be taken off-premises for the purpose of delivering healthcare services; this includes transporting records to visit patient's at home or travelling to another satellite location. In support of this, healthcare entities will need to adopt the appropriate safeguards to protect patient records to reduce the risk of unauthorized access or use while it is taken of the premises of the healthcare entity.

- ☐ Obtain approval prior to removal of patient records from the premises;
- ☐ Utilize a sign-out sysytem to document:
  - ☐ Who is removing the patient records
  - ☐ What type of patient records are being removed
  - ☐ When the patient records are taken and to be returned
- ☐ Remove patient records from the premises only when absolutely necessary;
- ☐ Retain original patient records, if possible;
- ☐ Remove the minimum amount of patient and records;
- ☐ Place patient records in secured folder, containers (e.g. safe), or location (e.g. car trunk);
- ☐ Refrain from viewing patient records in public (e.g. public place, public transit).

RISKCHECK
BY MARSH CANADA LTD.

Fall 2023

Summary

As healthcare entities take steps to adopt the appropriate safeguards to protect patient records under its custody, they will need to undertake a focused approach that involves employing the appropriate physical measures that addresses risks and exposures related to the access, storage, and usage of patient records. In doing so, they will be able to strengthen their posture but also ensure that they meet their respective ethical, professional, and legal obligations.