Personal Health Information Privacy & Security

Healthcare entities have the ethical and legal duty to protect personal health information (PHI) of its patients, which is defined as any identifying information in verbal, written, and oral form; it can include information related to physical or mental health, health history, health care services, health care plan, and payments or eligibility for health care. As custodians of PHI, healthcare entities need to adopt the appropriate measures to ensure the appropriate collection, use, and disclosure of PHI to maintain privacy and confidentiality.

As part of their overall approach to protect PHI, healthcare entities will need to consider its risks and address them through the implementation of a comprehensive risk management approach to prevent, mitigate, and transfer its risks. In doing so, they must take steps to strengthen their internal control system, as well build awareness across its organization to strengthen their due diligence to ensure compliance with laws and regulations and prevent any unauthorized access, use, or disclosure of PHI.

The following guidance highlights key areas of considerations for healthcare entities in regards to PHI privacy and security. 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. Governance

Having effective governance plays a vital role in establishing a culture that demonstrates its commitment to protecting all types of information across its organization, including PHI; this involves having the appropriate governance structure and measures to ensure the appropriate collection, use, and disclosure of PHI such that it fulfills its duties and obligations.

- ☐ Establish clear governance and management oversight on PHI privacy and security. Specifically, the oversight should aligned with the following:
  - ☐ Board of directors and/or board sub-committees;
  - ☐ Executive management; and
  - ☐ Business management.
- ☐ Establish clear management accountability on the advancement of the PHI privacy and security policy, program, and training. The accountability should rest with one of the following executive functions:
  - ☐ Highest level of management (e.g. the president or chief executive officer); and
  - ☐ Highest level of information management (e.g. the chief information or privacy officer)
- ☐ Establish clear criteria and channels for reporting matters related to PHI collection, use, and disclosure; review any legal obligations you may have as an employer and make sure you are aligned with them.
- ☐ Establish clear response and recovery measures when responding to PHI breach incidents; review any legal obligations you may have as an employer and make sure you are aligned with them.

2. Policies and Procedures

Establishing a policy and procedures is essential to ensure that PHI under its custody or control is collected, used and disclosed in accordance with relevant laws and regulations. As well, it should address the type of equipment and devices that should be used when handling and storing PHI and actions that need to be taken in response to a PHI breach.

- ☐ Develop and review, at least annually, a comprehensive suite of policies and procedures that address and provide guidance in the following areas:
  - ☐ Collection, use, disclosure, storage, and destruction of PHI;
  - ☐ Use of approved/encrypted and unapproved/unencrypted devices (e.g. laptops, phones); and
  - ☐ Management, investigation, containment, and remediation of a PHI breach.
- ☐ Each of the above policies and procedures should include but not limited to the following:
  - ☐ Commitment to safeguarding PHI across the organization;
  - ☐ Establishment of where the policy and procedures are enforced;
  - ☐ Articulates accountability of all parties:
    - ☐ Employees;
    - ☐ Independent practioners (e.g. physicians, midwives);
    - ☐ Volunteers;
    - ☐ Students; and
    - ☐ Vendors.
  - ☐ Articulates unacceptable behaviour (e.g. removal of PHI from premises);
  - ☐ Outlines training, including topics covered and frequency training will occur;
  - ☐ Outlines steps to filing a report, including mechanisms for reporting and required information;
  - ☐ Available support services internal and external to the organization;
  - ☐ Contact information of the person who is designated to receive complaints and/or inquiries.
- ☐ Ensure the policy is made available to all individuals and groups.

3. People

Ensuring that the appropriate culture of accountability is instilled across the organization will require healthcare entities adopt a comprehensive approach that is focused on its people delivering services on its behalf (e.g. employees, volunteers, vendors); this includes adopting the appropriate measures during the recruitment, on-boarding and training of its people to ensure they are positioned to succeed when working with PHI, including the appropriate collection, use, and disclosure of PHI to maintain privacy and confidentiality.

A. Job Desciption

- ☐ The following information should be supplied as part of the staff and volunteer job description; it should be tailored to meet the specific needs of the organization and outline the roles and responsibilities of the staff, volunteers and vendors, including duties when working with PHI.
  - ☐ Roles and responsibilities;

- ☐ Required/preferred skill(s) and experience(s); and
- ☐ Required/preferred license(s) and certification(s).

B. Screening

- ☐ Adopt mechanisms to screen potential hires for any previous history of working with PHI. The following screening controls should be in-place:
  - ☐ Job description declaration;
  - ☐ Application self-disclosure;
  - ☐ Reference checks;
- ☐ For all new hires and current staff, volunteers and vendors, keep complete records of the screening documents and ensure they are kept current, requesting new checks on a regular basis.

C. Interview

- ☐ The following practices can be adopted as part of the interview to assess fit and eligibility of candidates for staff, volunteers and vendor positions. The candidate shall be provided with the following:
  - ☐ Overview of the public entity and its mandate and services;
  - ☐ Roles and responsibilities of the staff, volunteers, and vendors,
  - ☐ Service or activity with which the staff, volunteers, and vendors will be involved; and
  - ☐ Accountability when during collection, use, disclosure, storage, and destruction of PHI
- ☐ The interviewer should ask the following types of questions which have been designed to gather specific information about the qualifications & experiences, which includes working with PHI. Below are the types of staff, volunteer, and vendor interview questions which can be asked as part of the process:
  - ☐ Competency interview questions;
  - ☐ Behavioural interview questions (past focused); and
  - ☐ Situational interview questions (forward focused).

D. Onboarding

- ☐ Require staff and staff to sign a confidentiality agreement that outlines their duties, duties, and requirements to uphold privacy and confidentiality when working with PHI;
- ☐ Require vendors to sign a confidentiality agreement that outlines their duties, duties, and requirements to uphold privacy and confidentiality when working with PHI. It can also impose additional requirements, which can include for the vendor to provide evidence of the following:
  - ☐ Established policies and procedures that upholds commitment to protecting and outlines measures used to collection, use, disclosure, storage, and destruction of PHI;
  - ☐ Established role-based mandatory training program that enhances awareness and understanding on their duties, obligations, and requirements when working with PHI;

- ☐ Established approach in investigating and management a PHI breach, including actions, timelines, and roles involved; and
- ☐ Appropriate insurance coverage for contract-related liabilities;

☐ Provide staff and volunteers with on-the-job training when initially assuming their duties. This can be achieved by appointing the following designated individual(s) to act as a resource:

- ☐ Manager or supervisor; and
- ☐ Peer resource.

☐ Provide staff, volunteers, and vendors with the opportunity to ask questions and seek feedback regarding their performance as it relates to carrying out their duties.

E. Training

☐ Develop a role-based mandatory training program that enhances awareness and understanding on their duties, obligations, and requirements when working with PHI. Specifically, the training should address the following:

- ☐ Definition and recognizing PHI;
- ☐ Consequence of non-compliance with policies and procedures;
- ☐ Reporting and responding to a PHI breach;
- ☐ Appropriate collection, use, disclosure, storage, and destruction of PHI;
- ☐ Measures in place to protect PHI across the organization.

☐ Establish a training schedule, which require new staff, volunteers, and vendors to receive training upon hire and current staff, volunteers, and vendors to receive refresher training at least annually.

4. Security

Having the necessary security measures in place will protect PHI in all forms (e.g. electronic, paper, verbal) throughout its life cycle across the organization and prevent any unauthorized collection, use, disclosure, storage, and destruction of PHI. The type of measures adopted will be appropriate to the sensitivity of the PHI and the nature of its use. The security measures that should be adopted by healthcare entities should include a blend of the following:

☐ Physical Measures

- ☐ Ensure that hardcopy PHI records are not left unattended/posted in plain view
- ☐ Requirement of locks for filing cabinets containing hardcopy PHI records
- ☐ Restrict access to offices and areas containing hardcopy PHI records
- ☐ Restrict hardcopy PHI records from being taken off premises

☐ Electronic/System Measures

- ☐ Standardized approval and review to grant system access
- ☐ Standardized approval and review to grant remote access
- ☐ Encyrpted e-mail, storage drive, and messaging technology
- ☐ Automated lockout of electronic devices due to inactivity

- ☐ Network and system access audits
- ☐ Completion of privacy impact assessment/threat risk assessment for new systems
- ☐ Requirement for use of strong passwords
- ☐ Requirement to change passwords to electronic devices at regular intervals

- ☐ Contractual Measures
  - ☐ Adopt a confidentiality/non-disclosure agreement with staff and volunteers;
  - ☐ Adopt a confidentiality/non-disclosure agreement with vendors, it should address;
    - ☐ Roles and responsibilities for collection, use, disclosure, storage, destruction of PHI;
    - ☐ Management of information security and privacy incidents and/or breaches; and
    - ☐ Training provided to its staff on information privacy and security.
  - ☐ Adopt a data sharing agreement with vendors; and
  - ☐ Require vendors to retain appropriate insurance coverage and limits.

Summary

To foster a culture that demonstrates its commitment to protecting all PHI under its custody, healthcare entities must take the appropriate measures to ensure the appropriate collection, use, and disclosure of PHI to maintain privacy and confidentiality. As part of this, it involves consideration of the range of privacy and security risks and the adoption of a comprehensive plan to strengthen its internal control system diligence to ensure compliance with laws and regulations and prevent any unauthorized access, use, or disclosure of PHI.