Preventing/Reducing Unauthorized Access to Personal Health Information
The health and safety of patients, and the quality of health care provided, are paramount considerations in hospital records management. Giving employees and other staff (as agents of health information custodians) quick and easy access to records of personal health information required for the delivery of health care services is essential, particularly when an individual requires urgent attention.

Hospitals are required to take reasonable measures to ensure that its agents do not abuse their access rights and privileges, and to ensure that they understand both their obligations to protect privacy and the security of personal health information and the consequences of failing to do so.

Since the introduction of the Personal Health Information Protection Act (PHIPA) in 2004, hospitals and other health information custodians have made tremendous strides to ensure that the privacy of individuals and the confidentiality of their personal health information remains a top priority.

Privacy breaches occur when personal health information in the custody or control of a hospital is collected, used, disclosed, retained or disposed of in a manner that contravenes PHIPA. This includes unauthorized access, such as when personal health information is viewed by a health care professional who is not providing, or assisting in the provision, of health care to the individual involved (usually a patient).

A privacy breach will have significant consequences for the individual, the hospital and the agent of the hospital.

Protection of privacy is a shared responsibility across all levels of an organization. Agents need to know that the hospital’s management and senior executive team are adamant about preventing unauthorized access – they take their responsibilities under PHIPA very seriously.

Together the Ontario Hospital Association and the Office of the Information and Privacy Commissioner have developed this resource to help hospitals ensure that they have a robust approach to preventing unauthorized access – one that is implemented consistently within and across their organizations.

Pat Campbell
President and CEO
Ontario Hospital Association

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Province of Ontario
The Ontario Hospital Association (OHA) and the Information and Privacy Commissioner of Ontario (IPC), have collaborated to develop this Primer for hospitals to highlight best practices for safeguarding personal health information (PHI) to prevent/reduce incidents of unauthorized access.

Specifically this Primer will:

- Define authorized and unauthorized access;
- Discuss the implications and consequences of unauthorized access;
- Outline ways your organization can prevent unauthorized access; and
- Describe how personal privacy should be protected in your organization.

The rules for the collection, use, disclosure, retention and disposal of PHI by health information custodians (e.g., hospitals) and their agents, (e.g., nurses, physicians, pharmacists and data entry clerks) are set out in the Personal Health Information Protection Act (PHIPA). PHIPA also provides individuals with a right to access their PHI, subject to limitations, and to request a correction of these records.

What is Personal Health Information (PHI)?

PHI is identifying information collected about a person, either orally or in writing. It includes information about an individual’s health or health care history in relation to:

- The individual’s physical or mental condition, including family health history;
- The provision of health care, including the identification of persons providing care;
- Long-term care services;
- Payment or eligibility for health care or eligibility for coverage for health care;
- Donation of body parts or bodily substances or information that is derived from the testing or examination of such parts or substances;
- The individual’s health card number; or
- The identity of a individual’s substitute decision-maker.

Identifying information includes health information that could identify an individual when used alone or in conjunction with other information. Identifying information about an agent of your hospital (e.g., employee) that is not maintained to provide care is not PHI.

PHI is among the most sensitive personal information about an individual. As such, the collection, use, disclosure, retention, and disposal of PHI requires a high level of protection by organizations and individuals who have such information in their custody or control.
Authorized Access to Personal Health Information

PHIPA provides that PHI is only permitted to be accessed for authorized purposes, including the collection, use and disclosure of PHI by health care professionals within an individual’s “circle of care.” While “circle of care” is not explicitly defined in PHIPA, it is commonly used to describe the ability of certain health information custodians to assume an individual’s implied consent to collect, use or disclose PHI for the purposes of providing health care.

The circle of care generally refers to those on the health care team who are actually involved in the care or treatment of a patient. Members of an individual’s circle of care can imply consent, or assume they have the individual’s implied consent, to collect, use and disclose the individual’s PHI for such care, unless the individual expressly withholds or withdraws consent.

Hospitals are required to take reasonable precautions to safeguard PHI from theft, loss and unauthorized use, and to notify the affected individual at the first reasonable opportunity if PHI is stolen, lost or accessed by an unauthorized person.

A privacy breach occurs whenever PHI in the custody or control of a hospital is collected, used, disclosed, retained or disposed of in a manner that contravenes PHIPA. This includes unauthorized use or access to PHI, such as when PHI is viewed by a health care professional where there is no health care requirement to view such information about that person.

Unauthorized Access to Personal Health Information

The IPC has issued a number of orders pertaining to unauthorized access. In two separate cases (H0-002 and H0-010), a hospital patient’s PHI was accessed by an employee of the hospital who was not providing care to the individual. In H0-010, the IPC ordered the hospital to undertake 10 remedial actions to prevent similar privacy breaches in the future.

Hospitals may learn about a privacy breach through internal reporting/auditing, when contacted by the IPC after a formal complaint has been received, or when the IPC investigates on its own initiative.

The Consequences of Unauthorized Access

A privacy breach in the form of an unauthorized access to PHI can have significant consequences for the individual, the hospital and the agent of the hospital (i.e., the hospital employee).

Consequences for the individual

A person whose PHI is accessed without authorization may be deterred from seeking testing or treatment in the future, and may withhold or falsify information provided to health care professionals for fear of unauthorized access. The unauthorized access of sensitive PHI may also result in the individual being discriminated against or stigmatized and may cause them economic or psychological harm.

Consequences for the hospital employee

Agents who access PHI without authorization may be subject to disciplinary action by the hospital at which they are employed, including a verbal warning, disciplinary letter, suspension or even termination. In addition, the actions of the agent may be reported to their licensing body or regulatory college which could have significant implications for the individual’s ability to work in the future.

For more information on circle of care see Circle of Care: Sharing Personal Health Information for Health-Care Purposes.
For example, the Ontario College of Nurses disciplined a member for unauthorized accesses of records of PHI. The affected individual was the ex-spouse of the member’s partner.¹

In addition to having her employment terminated, the member was found to have failed to meet the standards of practice of the College and to have engaged in conduct that would reasonably be regarded by members of the profession as dishonourable and unprofessional. The member had her certificate of registration suspended for six weeks and was required, for 12 months after the order was made, to notify all new employers of the decision, the order and the penalties imposed.

A breach may also result in prosecution by the provincial Attorney General. In Alberta, a medical office clerk pleaded guilty to charges of unauthorized access of another person’s PHI and was fined $10,000 by an Alberta court.

Consequences for the organization

A privacy breach may result in:

- Damage to the hospital’s reputation;
- An IPC order;
- Lost time and resources to contain, investigate, and remediate the breach;
- Prosecution by the Attorney General; or
- Legal action taken against the hospital.

The IPC’s two orders related to unauthorized access both garnered significant media and public attention and set out specific remediation that the hospital was required to complete.

In other provinces, the scope of repercussions has expanded outside of the privacy commissioner’s office. In early 2012, four class action law suits were brought against the Western Health Regional Health Authority, Eastern Health and Central Health in Newfoundland and Labrador for unauthorized access to PHI. While these cases have yet to be heard by the Newfoundland Supreme Court, the impact on the organizations, from a reputational and cost perspective, will likely be significant.

Preventing/Reducing Unauthorized Access: A Multi-Pronged Approach

As noted above, the consequences of a privacy breach can be devastating for individuals, hospitals, and agents of the hospital (i.e., hospital employees). Organizations should ensure they have a robust approach to preventing unauthorized access that is implemented consistently across the organization.

A privacy policy cannot, by itself, protect PHI. It must be operationalized throughout the activities of an organization.² Protection of privacy is a shared responsibility across all levels of an organization. Agents need to know that the hospital’s management and senior executive team are serious about preventing/reducing unauthorized access.

To prevent/reduce unauthorized access, the OHA and the IPC recommend this multi-pronged approach:

a) Education and Training

Organizations should ensure that all agents, including board-appointed professional staff with privileges, maintenance staff, and security staff, are appropriately trained upon hiring or upon the granting of access privileges. This training should be refreshed regularly (preferably annually). Education and training programs should include:

- An overview of role-based access rules, and the definitions of a privacy breach and unauthorized access;

---


• Details of the hospital’s planned response to unauthorized access, including a report to the employee’s regulatory college (where appropriate), and notice to the affected parties;

• Potential disciplinary action that the hospital will take in the event of unauthorized access;

• Notice that random audits will be conducted;

• Appropriate contact information for reporting privacy breaches; and

• Understanding the IPC’s role (i.e., a review of orders issued to date on unauthorized access).

New agents (e.g., employees) should be provided with copies of all privacy policies upon hire. Hospitals should consider building in confidentiality acknowledgments to initial employment contracts. Regular performance evaluations should include a renewal of confidentiality acknowledgments and build an obligation to protect privacy into the evaluation process.

b) Communications

Successful communications strategies can include:

• Log-on notices to staff asking them to acknowledge appropriate access and reminders about random audits;

• Posters with zero tolerance messaging, screensavers with reminders about privacy, fact sheets, and questions and answer documents;

• A confidential system for whistleblowers;

• Regular communications from Senior Management re-affirming a commitment to privacy (i.e., through newsletters, email, staff meetings); and

• Role-modeled commitment from Senior Management (i.e., attendance at training and education sessions).

Hospital privacy policies should be accessible and written in plain language. Employees should be aware of and commit to following these policies.

c) Importance of a Privacy Breach Protocol

Your organization should ensure that a written policy is in place for responding to all privacy breaches. Your organization’s privacy breach protocol should include:

• Zero tolerance of unauthorized access (both in policy and practice);

• Immediate temporary suspension of an individual’s access to records (and potentially employment) pending the outcome of an internal investigation;

• Policy on containment and notification of affected parties;

• Notice of the unauthorized access to your organization’s privacy officer, human resources department and the Information and Privacy Commissioner’s Office;

• Provision of all information regarding the breach and hospital’s response to breach to affected individuals;

• Discipline (where necessary and appropriate) following an investigation; and

• Process for conducting a full audit.

You can also refer to the IPC’s guidance document, What to do When Faced With a Privacy Breach: Guidelines for the Health Sector.

d) Audit and Evaluation

Hospitals need to ensure that auditing is in place for all systems containing PHI and that processes are in place to review system control and audit logs to prevent and identify unauthorized use or access to PHI.
Hospitals should be able to generate complete and accurate audit logs that identify:

- All agents who log-in to a system;
- Any and all user log-in identifications;
- All log-in attempts during a specified period of time and/or for a particular agent;
- Each agent who accessed an individual’s PHI through a specified period of time;
- Those individuals for whom an agent accessed PHI through the hospital during a specified period of time; and
- Any occasion on which the PHI for an individual who has requested restrictions (i.e., lockbox) was accessed and by whom.

When to conduct audits:

1. On a regular basis (monthly) with random patients, prominent patients when they are admitted and staff members when they are admitted;
2. Prior to any operational or technical changes to the electronic system or environmental circumstances impacting risk; and
3. In response to any suspected or actual privacy breach.