The Ottawa Hospital | L'Hôpital d'Ottawa

Sanction Guidelines for Privacy and Security Breaches

PURPOSE

The purpose of these guidelines is to recommend the sanctions for staff who violate The Ottawa Hospital's Privacy and Security Policies and the *Personal Health Information Protection Act (PHIPA)*.

Fair and consistent privacy and security policy enforcement and follow up action for those employees who breach patient privacy is critical to building trust in the organization, the sector, and the public. Each privacy incident or breach requires appropriate investigation along with managerial discretion to declare a violation or breach and institute a fair and reasonable response.

A breach means the unauthorized access, collection, use, disclosure or disposal of any personal health information and personal information. Breaches can be intentional (e.g. purposely accessing information on your ex-partner when you do not require such information for your job) or inadvertent (e.g. accidentally sending a report to the wrong fax number). Breaches also include a failure to protect personal information or personal health information with which an employee or agent is entrusted (e.g. leaving health records unattended, sharing passwords or discussing personal health information via social media). NOTE: Accessing one' own personal health information is not considered a privacy breach.

When imposing discipline for privacy breaches under levels two and three of the following guidelines, the standard application of progressive discipline levels will not apply, and suspension up to and including termination could result.

Categories of Privacy and Security Breaches

These categories define the significance and impact of the privacy and security breach to help guide corrective action and remediation steps:

Levels	Categories of Privacy and Security Breaches	Examples of Breaches	Disciplinary Action(s)*
1	Accidental or inadvertent This is unintentional	▪ Disclosing Personal Information (PI) or Personal Health Information (PHI)	▪ Counseling letter to employee (equivalent written communication to physician) outlining

	violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error.	without verifying identity of requestor. ▪ Leaving PI or PHI unattended in public areas. ▪ Failing to log off computer that holds PI and PHI. ▪ Inadvertently sending PI or PHI via fax, regular mail or e-mail to a wrong party.	TOH's expectations for protecting personal health information. ▪ Discussion/reinforcement of applicable policies and procedures. ▪ Consider reporting to applicable Regulatory College (i.e. similar breach). ▪ Privacy training ▪ Sign or re-sign confidentiality agreement.
2	Intentional, non-malicious This is a violation of policies or legislation surrounding the access, use and disclosure of PI or PHI.	▪ Accessing or using PI and PHI without professional need to know, or as part of the "circle of care". ▪ Discussion of PI and PHI with someone who does not have a legitimate need to know. ▪ Allowing another individual to use one's clinical systems (i.e. OACIS, PACS, SMS, etc.) user account or password. ▪ Accessing the information of high profile person or celebrity/media personality, including inappropriately viewing PHI beyond TOH's "VIP" flag ▪ Accessing or using PHI without a legitimate need to do so, such as checking a co-worker's health record. ▪ Posting PHI to social media web sites. ▪ Repeated Level 1	▪ If warranted under the circumstances, termination of employment or revocation of Medical Staff privileges may result. ▪ Suspension without pay for staff and suspension of Medical Staff privileges for physicians. ▪ Discussion/reinforcement of applicable policies and procedures. ▪ Privacy training ▪ Sign confidentiality undertaking and non-disclosure agreement. ▪ Report sent to applicable Regulatory College. ▪ Monitor and audit accesses on a regular basis.

		violation(s). ▪ Collecting PHI/PI for research purposes without prior REB approval ▪ Storing PHI/PI on an unencrypted USB key	
3	Intentional and malicious This is an intentional violation of policies or legislation for personal gain or to cause patient or organizational harm.	▪ Accessing PI and PHI without professional need to know for personal gain or to cause harm to another (i.e. using information for child custody dispute or divorce proceedings) ▪ Using another employee's computer account for personal gain or to cause harm to another. ▪ Intentionally altering data or removing PI and PHI in any form. ▪ Disclosing PI or PHI to an unauthorized individual or entity for illegal purposes (e.g. identity theft). ▪ Repeated Level 1 or 2 violations.	▪ Termination of employment (employee ineligible for future rehire) and access privileges removed. ▪ Revocation of Medical Staff privileges and access privileges removed. ▪ Report sent to applicable Regulatory College.

***Disciplinary Action (s) may be adjusted based upon the following Factors to be considered:**
Sanctions may be modified based on mitigating and/or aggravating factors. These factors may reflect greater damage caused by the violation and thus work against the violator, ultimately increasing the penalty.

Aggravating Factors:

- Violation of specially protected information such as HIV-related, mental health, substance abuse, and genetic data.
- High volume of people or data affected.
- Public relations impact on Hospital
- High liability exposure for the organization.
- Large organizational expense incurred, such as breach notification, conducting audits.
- Hampering the investigation, lack of truthfulness.

- Negative influence on others.
- History of other performance issues and/or violations.

Mitigating Factors: (The staff member has a responsibility for identifying mitigating factors that may lessen any potential penalty)

- Violator's knowledge of privacy and security practices (e.g. inadequate training, training barriers, or limited language proficiency).
- Culture of surrounding environment (e.g. investigation determines inappropriate practices in business unit).
- Violation occurred as a result of attempting to help a patient (with patient's consent).
- Victim(s) suffered no known financial, reputational, or other personal harm.
- Violator voluntarily admitted the violation in a timely manner and cooperated with the investigation.
- Violator showed remorse.
- Action was taken under pressure from an individual in a position of authority.

Accountabilities

Chief Privacy Officer/delegate and Information Security Officer are responsible to:

- Maintain current policies, standards, procedures, guidelines and tools required to support effective identification and management of privacy breaches.
- Implement, interpret and promote compliance with privacy policies including these guidelines.
- Appropriately educate and train staff with respect to compliance with TOH's responsibilities to protect privacy and the confidentiality and security of their PHI and PI in accordance with TOH's obligations under PHIPA, FIPPA and its internal policies and procedures.
- Investigate and confirm the violation, including assignment of level of severity, in collaboration with Human Resources and Manager.
- In collaboration with Human Resources, determine the appropriate sanction and corrective action, in conjunction with employee's Manager.
- Document the results of privacy breach investigations.
- Report the breach to the appropriate regulatory colleges, as applicable.
- Establish processes to promptly and regularly report privacy breaches and the results of any investigation to the President and CEO.
- Monitor the resolution of breaches and corrective action.
- Monitor and audit accesses on a regular basis.

Human Resources is responsible to:

- Document the results of breach investigations.
- Support the CPO and ISO in investigating breaches.
- In collaboration with the CPO/delegate, determine appropriate sanction and corrective action, in conjunction with employee's Manager. .

Medical Staff leadership is responsible to:

- Document the results of breach investigations.
- Support the CPO and ISO in investigating breaches.
- Determine appropriate sanction and corrective action in conjunction with CPO/delegate.
- Provide education and training to staff.

Manager/Director/VP is responsible to:

- Support the CPO and ISO in investigating breaches.
- Apply appropriate sanction and corrective action.
- Promote compliance with privacy policies including these guidelines in conjunction with CPO/delegate.
- Participate in education and training to staff.

Where there is no agreement as to the appropriate sanction, the President & CEO will make the final decision.