HNHB LHIN Privacy

Hamilton Niagara Haldimand Brant (HNHB)
Local Health Integration Network (LHIN)
Quality and Safety Committee

September 20, 2017

Ontario
Local Health Integration Network

Personal Health Information Privacy Act, 2004

- *Personal Health Information Privacy Act* (PHIPA) came into force on November 1, 2004
- The majority of PHIPA governs "**personal health information**" in the custody or control of **Health Information Custodians** and its **agents**.
- PHIPA also has broader application which would extend to non-health information custodians.

Duties Imposed on Health Information Custodians & their Agents

- A number of duties are imposed on health information custodians and their agents under PHIPA
- These duties generally fall into four categories:
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Responding to requests for access to and correction of records and personal health information
  - Transparency of information practices

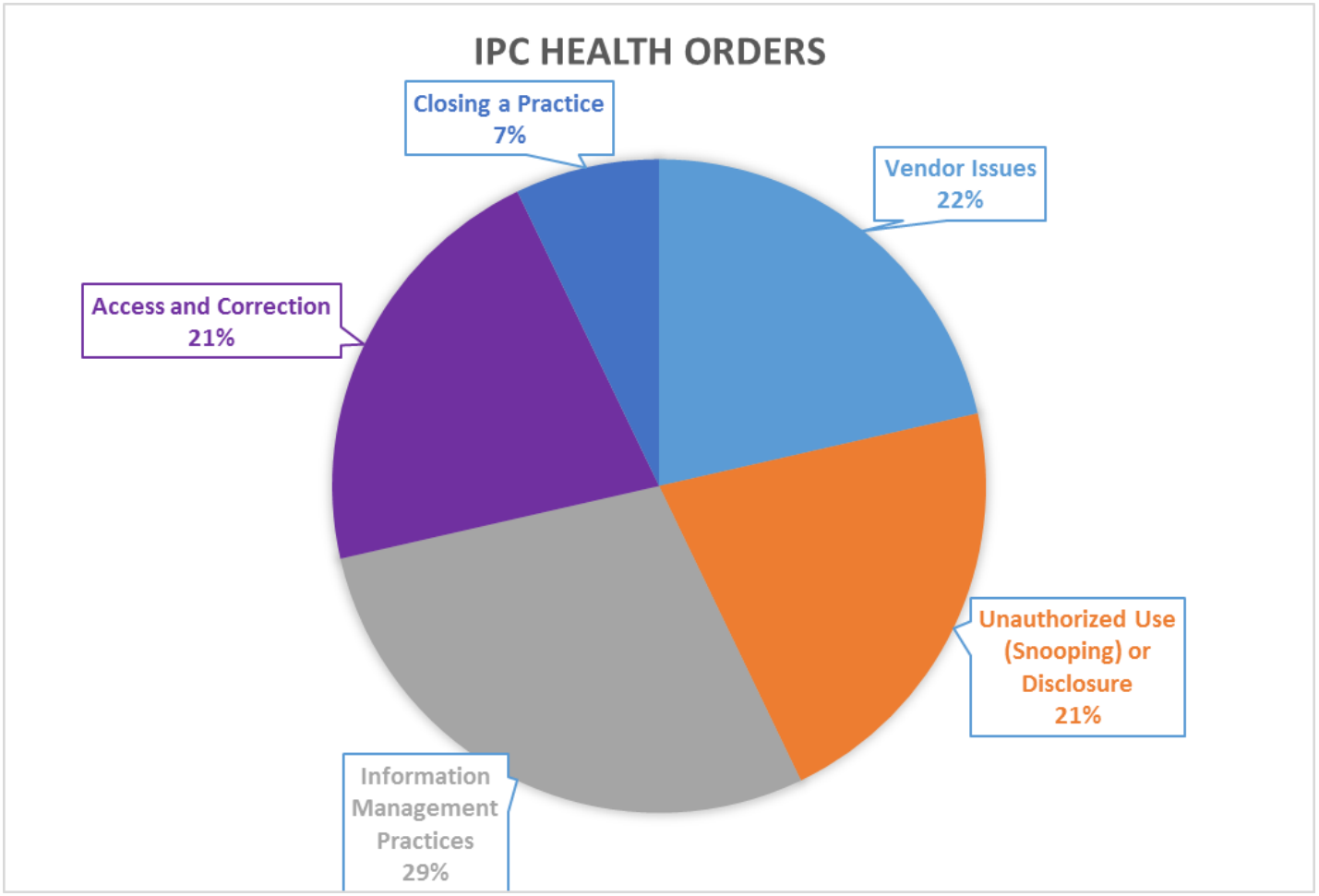
Bill 119- Health Information Protection Act, 2015

- The Bill was introduced on September 16, 2015
- All the provisions in the Bill relating to PHIPA were proclaimed into force on June 3, 2016, with the exception of Part V.1, which relates to the provincial electronic health record
- Consultation sessions on the new regulations have been underway throughout the summer of 2017 (target: January 1, 2018)

Bill 119- Health Information Protection Act, 2015 (continued)

- The provisions in the Bill include:
  - An amendment to the definition of “use” to clarify that viewing personal health information is a “use” under PHIPA
  - A new provision requiring health information custodians to take steps that are reasonable in the circumstances to ensure personal health information is not collected without authority
  - New provisions requiring notification of “Privacy Breaches”
  - Amendment to the provisions related to prosecution of offences under PHIPA

Information and Privacy Commissioner of Ontario (IPC)



Personal Health Information Protection Act
14 -Health Orders
49 -Decision

HNHB LHIN Response

Health Order	Description	Actions Taken
Vendor Issues HO-001 HO-006 HO-011	• Inappropriate destruction of information • Transfer of medical records between offices lost in mail.	• Agreements in place with bonded shredding company to properly destroy all paper records on site and off site storage locations. Health Order helped inform RFP requirements. • Electronic method to exchange personal health information with health care providers (HPG).
Unauthorized Use HO-002 HO- 010 HO-013	• Accessed medical records outside of the provision of care. • Lack of security features to identify sensitive files “VIP” warning • Accessed information and sold to RESP company	• CHRIS restricted “VIP” flags implemented • Standard Operating Procedure developed to audit patient records. • Increased on-going education to staff and implemented on-line module to reflect examples of snooping incidents.
Information Management Practices HO-004 HO-005 HO-007 HO-008	• Encrypted mobile device computer and USB- loss of information • Images from a surveillance camera intercepted	• Full disc encryption on all desktops and laptops • Acceptable use of technology policy

HNHB LHIN Response

Health Order	Description	Actions Taken
Access and Correction HO-009 HO-012 HO-014	• Recovery fee exceeded reasonable cost for access to records • Did not respond to request for records	• CCAC provincial guidelines developed to ensure costs are at or below the recommended fee schedule • Monitor and tracking system in place for access requests
Closing Practice H0-003	• Records abandoned when organization ceased to exist.	• Agreements outline expectations for record retention and permit the LHIN the right to request transfer of all records in the case an service provider ceases to exist.

HNHB LHIN Privacy Program

Accountability	• Designated Privacy Officer and Formal Back- Up Position • Policies and Procedures • Confidentiality • Agreements
Education and Awareness	• Robust New Employee Privacy Orientation (1 hr- Privacy Officer) • Privacy on-line module • Intranet Page dedicated to privacy
Monitoring and Compliance	• Event Management System to monitor privacy events • Privacy Impact Assessments • Auditing- Standard Operating Procedure • High Risk Reporting • Privacy Performance Report
Security	• Full Disc Encryption • User Terms and Conditions • Robust password protections • Audit logs
Transparency	• Privacy Statement on website • Privacy Brochures • Welcome packages • Consent module to capture informed implied consent model

Accountability

Privacy Officer

Health Information Custodians must designate a contact person (Privacy Officer) who is authorized to:

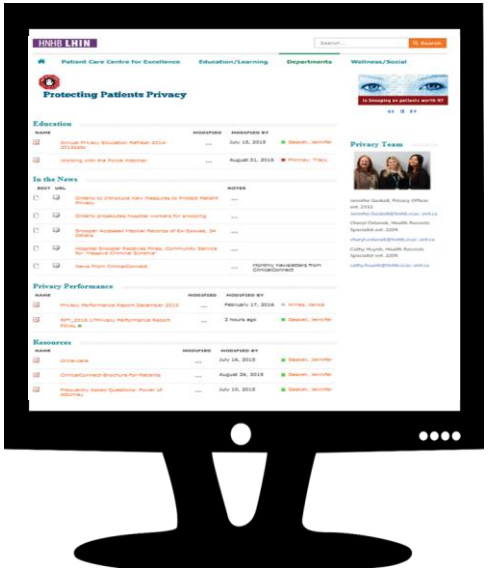
- Facilitate compliance with the Act
- Ensure all agents are appropriately informed of their duties
- Respond to inquiries in relation to information practices
- Respond to the requests of individuals for access to or correction of their records of personal health information
- Receive complaints about alleged contraventions of the Act

Agreements

- Data sharing, Network Sharing, Participant Agreements, Contributor Agreements
- Annual Attestations, Privacy Assessments, Breach Protocols, Auditing Expectation, Correction Protocols, Consent Directives, Committee participation

Education and Awareness

- New employee and annual privacy education materials reflect current trends in privacy breaches with a strong emphasis on snooping and acceptable uses.
- On-line module tracks completion rates
- Dedicated area on the intranet dedicated to privacy
- Privacy Officer on-going consultation



Monitoring and Compliance- Auditing

- Standard Operating Procedure for Auditing patient records:
  - Monthly Audits: same last name, random user, manual override, high user, user accounts
  - Human Resources is involved on all privacy investigation
  - All users are informed of audit and results

Monitoring and Compliance- Privacy Breach & Incidents

- Privacy Breach is when personal health information is stolen, lost or if it is used or disclosed without authority.
- Tracked in RL Solutions to reflect both Home Care and Service Provider Privacy Breaches and incidents
- Privacy Officer is alerted to all incidents through the system for both home care and service providers to action and follow-up
- Policy and Procedure in place which includes: immediately responding, containment, notification investigation and remediation
- Privacy reports generated to track trends

Future Steps regarding Privacy at HNHB LHIN

The Seven Foundational Principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into the Design
4. Full Functionality- Positive-Sum
5. End to End Security
6. Visibility and Transparency
7. Respect for User Privacy

Questions?