

Retention/Disposition of Patient Records - HIPA Obligations

Office of the Saskatchewan Information and Privacy
Commissioner

Diane Aldridge, Director of Compliance

Disclaimer

- Materials prepared are by the OIPC to assist persons in having a better understanding of the laws discussed.
- This information is only offered as non-binding, general advice. We cannot give advanced rulings.
- We are unable to discuss specific past or present cases, unless Report issued or details otherwise publicly known.

Role of OIPC

- ‘Umpire’ in the information age
- Independent Officer appointed by Legislative Assembly
- Oversees compliance by 3,000 + bodies in SK with 3 laws:
 - *The Freedom of Information and Protection of Privacy Act (FOIP)*
 - *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)*
 - *The Health Information Protection Act (HIPA)*

HIPA Oversight

- SK Information and Privacy Commissioner office
- Ombudsman model – no order making power
- Creates tools, resources for HIPA compliance
- E-newsletter – Saskatchewan FOIP FOLIO
- Own motion investigations (e.g. *Report on Misdirected Faxes from SK trustees*)

HIPA Overview

- Applies if :
 - (a) “Personal health information” (PHI)+
 - (b) “trustee” +
 - (c) “custody or control”
 - Consider extended reach for PHI under control of a trustee but not in the trustee’s custody [i.e. information management service provider (IMSP)]
- Comprehensive rules for:
 - Collection, use, disclosure, access & correction of PHI
- Designed to reflect many current practices and procedures

HIPA Overview (2)

- HIPA sets out 2 kinds of duties for trustees
 - **General duties**
 - [s. 9 (prospective transparency), 10 (retro transparency), 16 (policies and procedures), 22 (continuing duties), 23 (data minimization & need-to-know)]
 - **Transaction-specific duties**
 - Collection, use, disclosure, access, correction

Key Terms

- What is personal health information (PHI)?
 - Is defined by HIPA
 - Includes:
 - physical or mental health
 - health services provided to someone
 - donation of body part or substance
 - registration information [further defined by section 2(q)]
 - incidentally collected
 - Not PHI if sufficiently de-identified (means PHI from which any information that may reasonably be expected to identify an individual has been removed), aggregate or statistical

Other Key Terms

- **Privacy:** is a broad concept which involves the right of the individual to exercise a measure of control over his or her PHI. It involves the decision of the individual about what PHI will be disclosed to a trustee and for what purposes. Privacy captures both security and confidentiality which are subsets of privacy.
- **Confidentiality:** duty to prevent inappropriate use or disclosure of PHI
- **Security:** means employed to ensure that PHI is not inappropriately collected, used or disclosed

Adequate Safeguards

- HIPA prescribes that the trustee **must establish policies and procedures** to maintain **administrative, technical and physical safeguards**.
- These must **protect the integrity, accuracy and confidentiality** of the information.
- They must also **protect against any reasonably anticipated threat or hazard** to the security or integrity of the information; **and the loss of, unauthorized access to, use or disclosure** of the information

Retention & Destruction

- Retention & destruction policy

17(1) Not yet proclaimed.

(2) A trustee must ensure that:

(a) [PHI] stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information established in the policy mentioned in subsection (1); and

(b) [PHI] is destroyed in a manner that protects the privacy of the subject individual.

Retention & Destruction (2)

- **Continuing duties of trustees**

22(1) Where a **trustee ceases to be a trustee** ... the duties imposed by this Act on a trustee ...**continue to apply to the former trustee until** the former trustee transfers custody and control of the [PHI] to another trustee or to an [IMSP] that is a designated archive.

(2) Where a former trustee fails to carry out the duties continued pursuant to subsection (1), **the minister may appoint** a person or body to act in place of the former trustee until custody and control of the [PHI] is transferred to another trustee or to an [IMSP] that is a designated archive.

(3) Where a trustee dies, the duties imposed by this Act on a trustee ... become the duties of the **personal representative of the trustee** and continue to apply to the personal representative until the personal representative transfers custody and control of the [PHI] to another trustee or to an [IMSP] that is a designated archive.

Retention & Destruction (3)

- Designated archives

4(1) For the purposes of section 22 of the Act, the following are designated

archives:

- (a) affiliates;
- (b) the Department of Health;
- (c) health professional bodies that regulate members of a health profession pursuant to an Act;
- (d) [RHAs];
- (e) Saskatchewan Archives Board;
- (f) Saskatchewan Health Information Network;
- (g) University of Regina Archives;
- (h) University of Saskatchewan Archives.

(2) Nothing in this section requires a designated archive to accept [PHI] from a trustee.

THIS SLIDE INTENTIONALLY LEFT BLANK

Investigation Report (IR) H-2011-001

- On March 23, 2011, we were alerted to a large volume of patient files in a recycling bin in south Regina.
- 180,169 pieces of PHI (including approximately 2,682 patient files) in the recycling bin.
- Belonged to Albert Park Family Medical Centre (hereinafter APFMC). The responsible trustee was Dr. Teik Im Ooi.

IR-H-2011-001 (2)

- In total, 43 individuals were interviewed
 - eight of these individuals were interviewed multiple times.
 - included ten employees of APFMC and four employees of the pharmacy.
- Identified 11 key individuals that worked for six separate companies (see Schedule 3)
 - two of six companies had obligations under HIPA, and at least three were potentially functioning as an IMSP

IR-H-2011-001 (3)

- We learned that health records were **not shredded** since the opening of APFMC in 1993 until approximately 2010
- **No written agreement** between Dr. Ooi and IMSPs
- From 2007 until March 23, 2011 the large volume of patient PHI was **virtually unprotected**
- Approximately 150 boxes of patient records were moved from APFMC for storage purposes between 2005 and 2007, the discovery of files in the recycling bin leaves **unaccounted approximately 125 of those boxes** of patient records

IR-H-2011-001 (4)

- The Commissioner made 11 recommendations including:
 - within 30 days, provide our office with **comprehensive written policies and procedures** for the administrative and physical safeguards contemplated by sections 16, 17 and 18 of HIPA.
 - enter into **formal written agreements** with all existing IMSPs within 30 days and provide our office with copies.
 - each member of APFMC staff **execute a confidentiality undertaking** that includes an acknowledgement that breach of HIPA and APFMC privacy policies and procedures may be grounds for dismissal with cause.

IR-H-2011-001 (5)

- We offered guidance on what **elements** to include in an **IMSP contract**
 - Considered the Privacy Toolkit on both the CPSS and SMA websites, instruments and decisions from the Information and Privacy Commissioners from the provinces of Ontario and Alberta, COACH, College of Physicians and Surgeons of British Columbia and from Newfoundland and Labrador Health & Community Services

Consequences for Breach of HIPA

- HIPA Oversight
 - Commissioner's office
 - Power to investigate, require production of documents, take evidence under oath, etc.
 - Issue public reports naming trustee responsible
- Offence & penalty provision (s. 64 HIPA)
- Discipline by regulatory body
- Discipline by employer
 - CUPE (Local 3967) & RQHR
 - SEIU-West & Saskatoon RHA (St. Paul's)
 - Dismissals quashed and minor suspensions substituted
 - Implications

Advisory for Saskatchewan Health Trustees for Record Disposition

- Released April 12, 2011
- We therefore recommend that all trustees and trustee organizations IMMEDIATELY implement the following procedures:
 - Ensure that someone in the organization is **formally designated as the Privacy Officer** with specific responsibility for HIPA compliance, particularly the safe retention and disposition of PHI.
 - Ensure that the trustee organization has **written policies and procedures** as prescribed by section 16 of HIPA including physical, administrative and technical measures reasonable for the protection of PHI.
 - Ensure that **every person in the trustee organization understands** the difference between the historic culture of confidentiality and the new requirements of HIPA including the **continuing responsibility for patient files** pursuant to section 22 of HIPA.
 - Ensure that the trustee organization is in **compliance with the transparency obligations** in sections 9 and 10 of HIPA.

Advisory (cont'd)

- Ensure that there is a **proper record retention and disposition schedule** and that it is followed.
- Ensure that all PHI is **properly and safely stored** at all times.
- Ensure that when disposing of personal health information all materials are **shredded or otherwise completely destroyed**.
- Ensure that if the storage or destruction of patient files is outsourced or if an IMSP is involved that there is a **proper agreement** that complies with sections 16, 17 and 18 of HIPA.

To be HIPA Compliant

- (a) A specifically **tasked privacy officer** with a clear mandate and appropriate training;
- (b) **Extensive training** of staff in HIPA requirements and provisions;
- (c) **Comprehensive, clear and practical written policies and procedures** that are reinforced through leadership and training of staff;
- (d) **Written contracts** with IMSP's that specifically address the requirements of section 17 and 18 of HIPA;
- (e) **Audit of use and disclosures** of the PHI; and
- (f) Effective **enforcement action** to follow any breach.

Resources (1)

- From Saskatchewan:
 - *Welcome to the Brave New World of Electronic Health Records* (Sk. CBA Mid-Winter Conference, Feb. 4, 2011)
(<http://www.oipc.sk.ca/Presentations/CBA%20Mid-Winter%20Conference%202011.pdf>)
 - OIPC Investigation Report H-2011-001
(<http://www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf>)
 - OIPC Investigation Report H-2010-001
(<http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf>)
 - Glossary of Common Terms – HIPA
(<http://www.oipc.sk.ca/Resources/HIPA%20Glossary%20-%20Blue%20Box.pdf>)

Resources (2)

- From Saskatchewan (cont'd)
 - OIPC Annual Report 2010-2011
(<http://www.oipc.sk.ca/Annual%20Reports/2010-2011%20Annual%20Report%20-%20FINAL.pdf>)
 - OIPC Annual Report 2009-2010, pages 20-26
(<http://www.oipc.sk.ca/Annual%20Reports/Annual%20Report%202009-2010%20FINAL.pdf>)
 - OIPC Annual Report 2008-2009, pages 26-30
(http://www.oipc.sk.ca/Annual_Report_2008-2009.pdf)

Resources (3)

- From the Canadian Medical Association (CMA):
 - *Principles for the Protection of Patients' [PHI]*
(<http://www.cma.ca/policybase>)
 - *Data Sharing Agreements: Principles for Electronic Medical Records/Electronic Health Records*
 - *Physician Guidelines for Online Communication with Patients*

Resources (4)

- From Canada Health Infoway:
 - *White Paper on Information Governance* (http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf)
 - *Conceptual Privacy Impact Assessment* (http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf)
 - *Infoway's Privacy Mandate*
(<https://www.infoway-inforoute.ca/lang-en/about-infoway/vision/privacy-mandate>)

Resources (5)

- From Alberta:

- 1) PIA Requirements –

<http://www.oipc.ab.ca/pages/PIAs/PIARequirements.aspx>

- 2) HIA Guide -

http://www.oipc.ab.ca/Content_Files/Files/Publications/HIA_Guide_August_2010.pdf

- 3) Netcare Investigation Report -

<http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2256>

- 4) AHW Netcare website link - <http://www.albertanetcare.ca/>

- 5) AHW Guidelines Manual - <http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf>

- 6) CPSA – Data Stewardship Framework -

http://www.cpsa.ab.ca/Libraries/Res/CPSA_Data_Stewardship_Framework.sflb.ashx

Resources (6)

- From Ontario:

1. Toolkit for doctors making the transition from paper-based to electronic records -- <http://www.ipc.on.ca/images/Resources/hipa-toolforphysicians.pdf>
2. Order HO-002 -- Ottawa Hospital breach -- http://www.ipc.on.ca/images/Findings/up-HO_002.pdf

- From British Columbia:

- OIPC Investigation Report F10-02
(http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-02.pdf)

Questions??

- Saskatchewan Information and Privacy Commissioner
 - Phone: (306) 798-1602
 - Toll free: 1-877-748-2298
 - Fax: (306) 798-1603
 - Email: daldridge@oipc.sk.ca
 - Website: www.oipc.sk.ca