Privacy Training for FHT Boards

Association of Family Health Teams of Ontario

Kate Dewhirst

February 3, 2016

DDO HEALTH LAW

Question 1

In a FHT/FHO* relationship, who is the “Health Information Custodian”?

DDO HEALTH LAW

PHIPA Applies to:

- **"Health information custodians"** (HICs) that collect, use, and disclose personal health information (PHI) [The FHT or FHO* - see new AFHTO tool]

- "**Agents**" of HICs (incl. employees, physicians, allied health professionals, vendors, students and volunteers acting on behalf of a HIC)

Who are Health Information Custodians?

- Health care practitioners*(including group practices likes FHTs and FHO*s)
- Public hospitals
- Private hospitals
- Psychiatric facilities
- Independent health facilities
- CCACs
- Community health or mental health centres, programs or services (primary purpose is provision of health care)
- Long-term care homes
- Placement coordinators
- Retirement homes
- Pharmacies
- Laboratories
- Specimen collection centre
- Ambulance services
- Operators of care homes (residential tenancies)
- Homes for special care
- Community support services provider (under *Home Care and Community Services Act, 1994)*
- Minister of Health and Long-Term Care
- HCCA evaluators or SDA assessor
- Medical Officer of Health
- Or as prescribed

HICs

- A health care practitioner or a person who operates a group practice of health care practitioners
- Who is the HIC?
  - Usually is the FHO* (or individual physicians)
  - The HIC has all the responsibilities under PHIPA (some duties can be delegated)

Question 2

What do HICs have to do?

DDO HEALTH LAW

AFHTO Statutory Compliance

- Duty: As a health information custodian (or agent), every FHT has a duty to protect personal health information
- Questions the Board should ask:
  - Are we a HIC? Or are we an agent of a HIC (being the FHO* or our affiliated physicians)?
  - Does the FHT have a Privacy Officer?
  - What steps has the FHT taken to ensure that it is PHIPA compliant?

AFHTO Statutory Compliance

- How does the FHT ensure and monitor third party access to personal health information?
- When was the last review/audit of the FHT's privacy policy and/or procedures?
- When did the FHT last train the staff on privacy issues?
- Has the FHT had any privacy breaches? If so, what steps have been taken to prevent recurrence?

Privacy Compliance Elements

1. Appoint a privacy officer
2. Post information management practices (staff/patients/public)
3. Have clear rules about privacy (usually in policy)
4. Ensure agents are informed about their duties under PHIPA (training)
5. Respond to public inquiries
6. Respond to requests for access/correction to a record of PHI
7. Perform Privacy Impact Assessments for new technology
8. Audit for compliance
9. Receive and respond to complaints
10. Take reasonable steps to ensure accuracy of PHI
11. Ensure protection of PHI against loss, theft, unauthorized access, use or disclosure, copying, modification, disposal (and notify affected individuals if there has been a privacy breach)
12. Ensure that records of PHI are retained, transferred and disposed of in a secure manner

Privacy Compliance Status

Requirement	Status	Notes
Privacy Contact Person		
Statement of information management practices		
Privacy policies		
Training for agents		
Process for responding to requests for access/correction		
Process for responding to privacy complaints/breaches		

Privacy Compliance Status

Requirement	Status	Notes
Privacy impact assessments for new technology		
Audit for compliance		
Contracts with vendors supplying IT services, confidential shredding and off-site storage reviewed		
Information security strategy		
Fees		
Confidentiality pledges		
eMR privacy flags + privacy reminders		

Question 3

What privacy laws, rules and resources do FHTs/FHO*s need to know about and review?

DDO HEALTH LAW

Privacy Rules for FHTs

- PHIPA
- Information & Privacy Commissioner of Ontario Orders – now there are 22
- College guidelines
- Organizational Policies – such as:

  (1) Privacy Policy; (2) Public Privacy Statement; (3) Safeguards; (4) Lockbox; (5) Privacy Breach Protocol; (6) ROI – Access and Correction; (7) Privacy Impact Assessment

Question 4

Why should the Board care about the privacy legislation? What impact could it have on the FHT? What are the penalties?

DDO HEALTH LAW

Consequences for Breach of Privacy

- Personal cost to patients and therapeutic relationship
- Individuals may complain to FHT and then to Privacy Commissioner (IPC)
- IPC has power to initiate investigations and has broad order-making powers
- **Damages for breach of privacy in court (class actions)**
- Offences with fines of $50K/$250K **(Bill 119 – at second reading - would double these fines and require reports to IPC/O & Colleges)**
  - **Prosecutions by Attorney General**
- Regulatory Colleges have power to take disciplinary action
- Employer can take disciplinary action including termination of employment or contract

Question 5

What privacy rights do patients have?

DDO HEALTH LAW

Individual Rights under PHIPA

Subject to some exceptions, an individual has a:

- Right to consent (or withhold or withdraw consent) to the collection, use or disclose of PHI
- Right to have access to PHI (regardless of where it is kept)
- Right to ask for a correction to a record of PHI
- Right to “lock” PHI from health care providers for health care purposes (“lockbox”)
- AND OTHER RIGHTS

Question 6

What happens if PHI is lost, stolen, accessed by someone inappropriately?

Lost, Stolen or Unauthorized Uses and Disclosures

- A HIC is required to notify the person if his or her information is lost, stolen or used by or disclosed to an unauthorized person
- FHT/FHO* staff must notify the Privacy Officer if this happens
- After Bill 119 – likely will also need to report to IPC

Security is a HUGE issue

- Fax with test results is misdirected
- An unencrypted laptop with health information saved on the hard drive is stolen
- An unencrypted USB key is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- Health records are recycled and not shredded
- Out of curiosity, a staff member reviews an ex-boyfriend's chart
- Staff send an email with patient data to a "help desk" – but send to the help desk at a bank
- Student looks through eMR for self-initiated educational purposes and not as directed by the instructor or preceptor

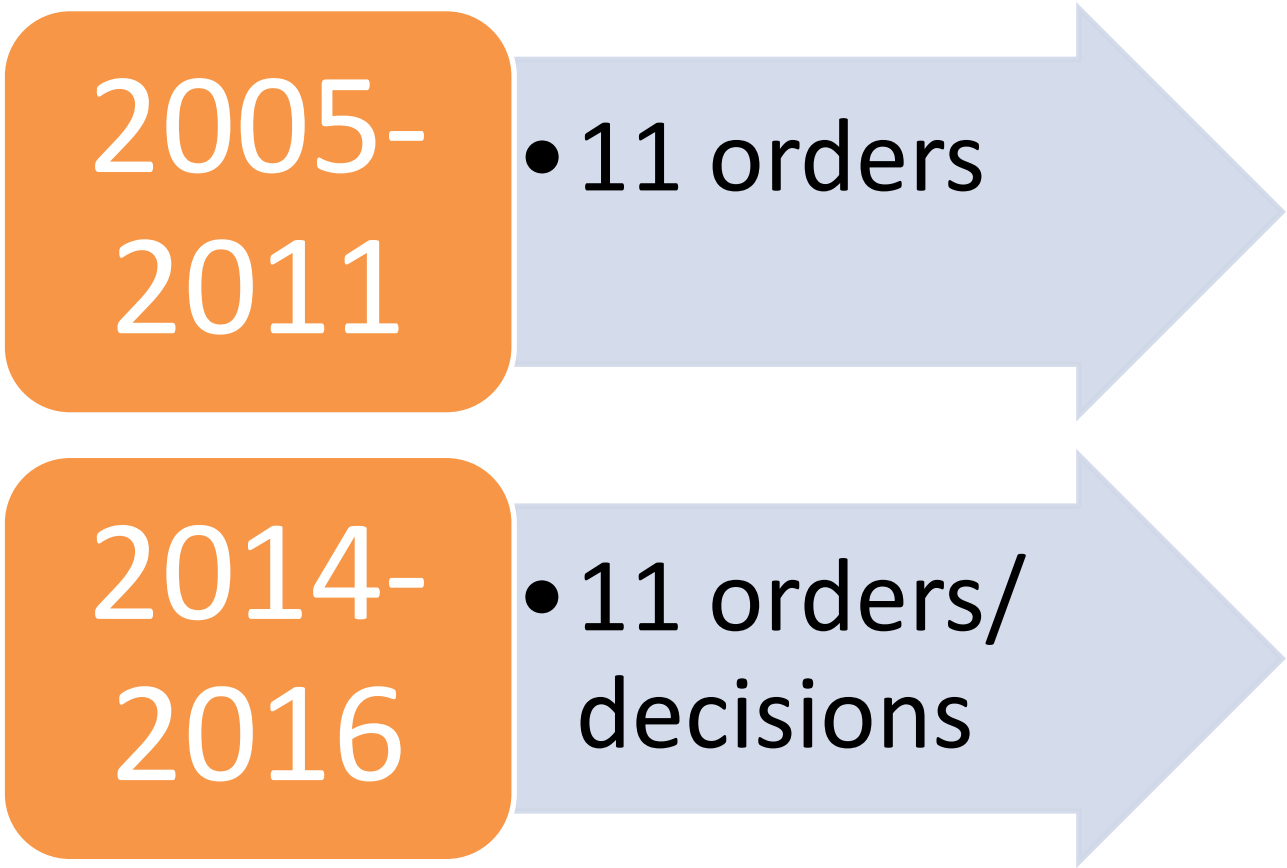
- A staff member makes a copy of an ex-spouse's health record
- Staff discuss patients in hallways and lunchrooms and other patients overhear (even colleagues overhear)
- Staff release information to another health care provider when a patient has said she doesn't want that provider to know
- Staff release information to a spouse when the patient doesn't want that spouse to know
- Staff release information to a child's parent when the child is capable of making his own decisions and said don't tell my parents

Question 7

Are there privacy practice standards that FHTs/FHO*s should know about?

DDO HEALTH LAW

IPC Orders and Decisions



IPC Orders Themes

Vendors

Orders 1, 6, 11

Snooping

Orders 2, 10, 13, 16

Mobile Devices and New Technology

Orders 4, 5, 7, 8,

Access and Correction

Orders 9, 12, 14, 15, 17, 18

Closing a Practice

Order 3

Disclosing Records of Deceased

Orders 19-22

Dealing with Vendors

DDO HEALTH LAW

Real Life Privacy Breaches

- **Order #1** – PHI on streets as part of film shoot
- **Order #6** –PHI scattered on the street outside medical centre with medical lab
- **Order #11** – CCO couriered Screening Reports but they never arrived

Real Life Privacy Breaches

- Review physical storage policies and procedures
- Have written contracts with third parties that transport, retain, destroy PHI
- Confetti shredders
- Reminder: Look at contracts with vendors for shredding
- Do PIAs – for all new initiatives and technology

Closing a Practice

DDO HEALTH LAW

Real Life Privacy Breaches

Order #3 – Medical clinic abandons records when it closes

- Duty to address records when closing a practice or retiring or moving
- CPSO has guidelines
- Be careful when renovating offices

Snooping

Real Life Privacy Breaches

- **Orders #2 & 10 (same hospital)**
  - Inappropriate access by employee to PHI of boyfriend's "ex" (#2) and former husband's wife (#10)
    - Instill a "culture of privacy"
    - Implement safeguards (lockbox) when patient presents concerns
    - Prompt investigations and remedial action
    - Role-based access

Real Life Privacy Breaches

Order #13

- Selling of information about new mothers and new babies to RESP providers
- Securities Commission fine: $36K + $9K to victims' fund
- Also linked to Securities Commission prosecution + class action ($400 million possibly 14,000 patients affected)
- Reminders:
  - Training
  - Audits (even when outside your control)
  - Policies
  - Confidentiality pledges

Recent Recommendations from IPC/O

- Annual confidentiality pledges
- Monthly random audits of electronic medical records to monitor for privacy breaches and inappropriate access to patient records
- Flag (to the extent that it is possible) likely targets of inappropriate access by staff (such as family members of FHT staff and high-profile individuals in the community)
- Privacy warning to the electronic medical record to pop up automatically upon log-in
- Privacy training should be repeated on a yearly basis to include IPC/O videos, in-house privacy training and different speakers

Real Life Privacy Breaches

- Jones v. Tsige, 2012
  - Bank employees
  - Tsige has common law relationship with Jones' ex
  - Tsige looked at Jones' financial information 174 times in 4 years
  - $10,000 damages (but the Court said, up to $20,000 for new tort of intrusion upon seclusion)

Jones, cont'd

- An ***unauthorized*** intrusion;
- The intrusion was **highly offensive to a reasonable person**;
- The matter intruded upon was **private**; **and**
- The intrusion **caused anguish and suffering** (although the Court suggests this last one will be assumed when the first three are satisfied)

Hopkins v. Kay 2015

- The respondent, Erkenraadje Wensvoort, was one of 280 patients who had their health information improperly accessed and who were notified of the breach, as is required by *PHIPA*.
- The respondent had previously sought medical care for injuries inflicted by her ex-husband, whom she had subsequently left and hidden from. She feared that the breach was actually an attempt by him to locate her.
- Hospital admitted privacy breach and said it was intentional
- Individuals have a right to sue outside the scheme set out in PHIPA
  - PHIPA says plaintiffs can sue after the IPC/O issues an order and then only for "actual harm"
  - Court recognized Jones v. Tsige (not required to prove actual harm and quantum of damages is higher than allowed under PHIPA)
  - HICs now potentially exposed to greater damage awards (+280 plaintiffs!)
  - No good faith immunity
- Decision upheld by Court of Appeal in 2015 and SCC has refused to hear an appeal so the decision stands
- Class action free to proceed

Real Life Privacy Breaches

Decision #16

- IPC refused a doctor's request to defer the IPC's review until the CPSO investigation has concluded
- Former patient of a medical clinic alleges that her ex-spouse obtained her medical records from the clinic and from the hospital without her consent (he was not her health care provider)
- She alleges he gained access to the records through deception and then shared the records in a court proceeding
- IPC concluded that because:
  - The CPSO investigation may not resolve quickly
  - There was no evidence of prejudice to the respondent physician (other than inconvenience in responding to two proceedings)
  - Orders and recommendations are different b/c IPC and CPSO
  - The CPSO outcome would not narrow the issue at hand for the IPC

Snooping Prosecutions

- North Bay nurse looked at 5804 patient records – case dropped by Attorney General because of delay of process (16 months)
- 3 hospital staff members are being prosecuted for privacy breaches involving a high profile patient
- Charges have been laid involving a student looking at records at a medical clinic

Arbitration case

Ontario arbitration *North Bay Regional Health Centre* 2012

- Nurse looked at 5804 patient records – case dropped by Attorney General because of delay of process (16 months)
- Daily review of health records out of personal interest and "learning"
- Her termination of employment was upheld by arbitrator

Snooping Video

45 minute video: https://www.youtube.com/watch?v=2DddxHvJPcY

Portable Devices and Technology

DDO HEALTH LAW

Real Life Privacy Breaches

Order #4 - Theft of laptop computer containing PHI of 2900 patients

- Develop “a comprehensive corporate policy that, to the extent possible and without hindering the provision of health care, prohibits the removal of identifiable PHI in any form from the hospital premises. To the extent that PHI in identifiable form must be removed in electronic form, it must be encrypted.”
- TAHSN Guidelines

Real Life Privacy Breaches

Order #7

- USB key lost by public health nurse going to flu immunization clinic
- More than 80,000 patients affected
- See order #4
- “Encrypt your mobile devices: Do It Now”
- “Strong encryption”

“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”

Real Life Privacy Breaches

Order #8 – But it happened again

- Stolen laptop – not encrypted
- More than 20,000 patients affected
- Incident reports, operating room lists, research data sets, class lists for patient education sessions (no health numbers or patient addresses)
- See orders #4 and #7
- Corporate policy re mobile devices
- Training
- Encryption

Real Life Privacy Breaches

Order #5 – Wireless camera in bathroom of methadone clinic

- If using wireless technologies, must be scrambled or encrypted
- Review practices and technologies regularly
- IPC fact sheet on wireless technologies released

Access and Correction

DDO HEALTH LAW

Real Life Privacy Breaches

Order #9 – Fees charged to access health records must be reasonable

- Physician could only charge $33.50 not $125 for 34 pages of psychological therapy notes
- Not cost recovery
- There are draft fee regulations – those should be followed

Real Life Privacy Breaches

Order #12 – Organization refused patient access to health record (deemed refusal)

- Must respond to requests for access to health records within 30 days

Real Life Privacy Breaches

Order #14 – Fees charged to access health records must be reasonable

- London Health Sciences charged $117 to a lawyer
- $117 was above and beyond “reasonable cost recovery”
- Could only charge $53
  - $30 to process the request + copies of the first 20 pages
  - + $0.25/page for the remainder

Real Life Privacy Breaches

Decision #15

- Psychologist providing an assessment for a Custody and Access Assessment Report
- One parent wanted psychologist to “correct” report
- Held: Psychologist was NOT a HIC for the purposes of this report and did not have to correct it b/c obligations of a HIC did not apply
- A regulated health professional who is not providing health care to a client is not a HIC for the purposes of PHIPA
- Hooper v. College of Nurses of Ontario + Wyndowe v. Rousseau

Real Life Privacy Breaches

Decision #17

- FIPPA and PHIPA
- Mackenzie Health (formerly York Central Hospital)
- An infant died shortly after birth – husband/father asked for records
- Raises issues of the interplay between FIPPA and PHIPA
- What is “personal health information”?
- Under what circumstances can organizations not disclose records to a requester?
  - What does it mean if you are subject to FIPPA and PHIPA? (like hospitals)
  - What does it mean if you are only subject to PHIPA?

Real Life Privacy Breaches

Decision #18

- Sensenbrenner Hospital
- A mother asked for her son's records after he died in a fatal car accident
- She believed the hospital should have more records than she was given
- What constitutes a "reasonable search"?
- IPC dismissed the complaint and said hospital did a reasonable search

Disclosure of Deceased Person's Records to Someone Other than Estate Trustee

DDO HEALTH LAW

Real Life Privacy Breaches

- 4 new decisions released
- Generally about family members who wish to have information about deceased persons (and estate trustees refused to share info)
- HICs must consider whether to exercise their discretion to disclose under s. 38(4)(b) or (c)
- IPC cannot require the disclosure – but can order HICs to consider and ensure HICs only contemplating relevant factors in their decision making

Real Life Privacy Breaches

s. 38(4) A HIC may disclose PHI about an individual who is deceased, or is reasonably suspected to be deceased:

a) For the purpose of identifying the individual
b) For the purpose of informing any person whom it is reasonable to inform in the circumstances of:
    a) The fact that the individual is deceased or suspected to be deceased and
    b) The circumstances of death where appropriate
c) To the spouse, partner, sibling or child of the individual if the recipients of the information reasonably require the information to make decisions about their own health care or their children's health care

Social Media

DDO HEALTH LAW

Real Life Breaches

Ontario arbitration *Credit Valley Hospital* 2012 (Brathwaite)

- Employee posted pictures on Facebook of a patient who committed suicide in a hospital parking lot (age and location of patient were revealed in the posting)
  - Should have known possibility that it was a patient (even though off site)
  - Employee was not remorseful
  - Not a momentary lapse in judgment - time elapsed between the posting of the two photos, and then the related commentary
  - Deterrence message was important

Real Life Breaches

Chatham-Kent v. CAW 2007

- Employee blogged about nursing home residents and co-workers
- Only used first names but pictures of staff and residents were uploaded
- Employee worked at the facility for 8 years, she apologized but she was terminated and that decision was upheld by an arbitrator
- The arbitrator found that the postings amounted to insolence and a grave breach of confidentiality

Privacy Training for Staff

1. Am I allowed to leave a voice message for patients with health information?
2. Can a patient's spouse make an appointment over the phone?
3. Do I have to share information with a teenager's parents? Am I allowed? What age can kids make their own decisions about their information?
4. What do we do when staff are patients here?
5. Are we allowed to look at our own health records? What about our children's health records?

Privacy Training for Staff

6. What do I do when a patient of the FHT comes up to me at the grocery store?
7. Can I give specialists and diagnostic services appointment information?
8. Can I give PHI in response to letters from lawyers, criminal investigations, insurance companies?
9. Do I have to give copies of tests and results and consult notes to patients at the end of their appointment?
10. What is the circle of care? Are we allowed to share information with the hospital? School? CAS? Police? HealthLinks?

Privacy Training for Staff

11. Is it a breach if someone overhears another person's health information (like diagnosis)?
12. Should we have privacy windows that slide in reception?
13. Should staff use patient numbers instead of patient names when calling into a room?
14. Can support staff scan reports for urgent results?
15. Can we use email to communicate with patients/other health care providers? (text message?)

Privacy Resources

- Association of Family Health Teams of Ontario
  - Privacy Toolkit for the Quality Improvement Decision Support Program in Family Health Teams
  - Statutory Compliance Toolkit for Boards of Family Health Teams and Nurse Practitioner-Led Clinics
  - Top 5 Privacy Questions Answered with 5 Privacy Tools

Privacy Resources

- Information and Privacy Commissioner of Ontario
  - 45 Minute PHIPA Training Video for all health sector staff
  - PHIPA Fact Sheets
  - PHIPA Orders
- College of Physicians and Surgeons of Ontario
  - Confidentiality of Personal Health Information
  - Medical Records
  - Appropriate Use of Social Media by Physicians
- College of Nurses of Ontario
  - Confidentiality and Privacy – Personal Health Information
  - Social Media

Privacy Resources

- Canadian Medical Protective Association
  - Privacy and Confidentiality
  - Documentation
- Ontario Hospital Association and Ontario Medical Association
  - Hospital Privacy Toolkit
- OntarioMD
  - Privacy & Encryption Online Tutorial
- DDO Health Law
  - 3 day Privacy Officer Training for the Health Sector
  - 3 hour Privacy Training for Family Health Teams
  - 1 hour Privacy Training for the Health Sector (online streaming video) – Coming March 2016
  - Legal Issues for Family Health Teams Monthly Teleconference

Privacy Training for FHT Boards

Kate Dewhirst

kdewhirst@ddohealthlaw.com

Follow me on Twitter: @katedewhirst

Check out our website and blog:
www.ddohealthlaw.com

Coming soon (March 2016):

www.thehuddleseries.com online videos

DDO HEALTH LAW