G2G Session: Privacy and Data Security

March 31, 2015

Please enjoy something to eat and introduce yourselves to others seated at your table.
The session will begin at 6 p.m.

Agenda

Agenda Item and Lead	Purpose	Time
Welcome *Ron Haines* Vice Chair, Mississauga Halton LHIN		6:00 – 6:03 p.m.
Introduction of Robin Gould-Soil *Ron Haines* Vice Chair, Mississauga Halton LHIN		6:03 – 6:05 p.m.
Privacy and Data Security *Robin Gould-Soil* Director Privacy and Access, and CPO, University Health Network	Education and Sharing of Ideas	6:05 – 7:05 p.m.
Break	15 minutes	7:05 – 7:20 p.m.
Questions and Answers *Robin Gould-Soil* Director Privacy and Access, and CPO, University Health Network	Education, Engagement and Consultation	7:20 – 7:55 p.m.
Closing Remarks *Ron Haines* Vice Chair, Mississauga Halton LHIN		7:55 – 8:00 p.m.

Welcome and Introduction

Ron Haines
Vice Chair,
Mississauga Halton LHIN Board of Directors

Privacy and Data Security

Robin Gould-Soil

Director, Privacy and Access and Chief Privacy Officer

University Health Network

PHIPA

- Ontario's ***Personal Health Information Protection Act*** defines how personal health information must be handled.
  - PHIPA builds on other laws, like the Public Hospitals Act, in setting out obligations for all staff, students and volunteers working on behalf of the Health Service Provider to protect patients' personal health information.

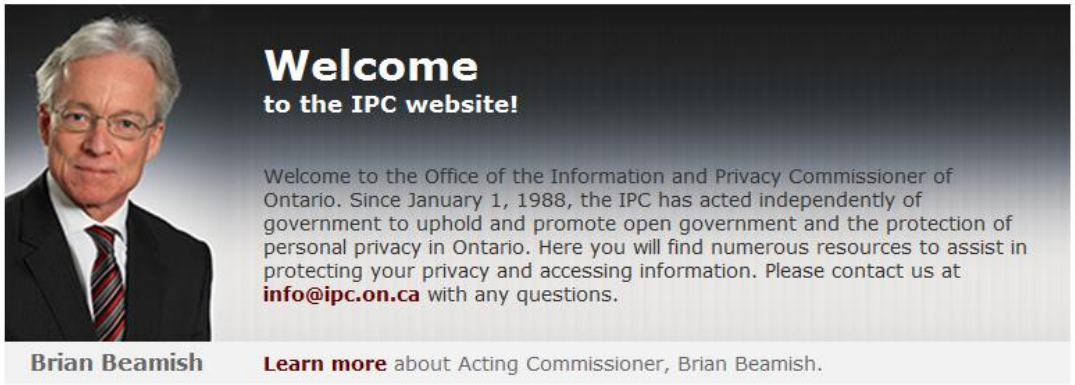
- What is personal health information (PHI)?
  - PHI is any information about an individual that identifies them and connects them to receiving care at Health Service Providers

- PHI can be found in many forms, including:
  - papers (e.g. charts, printouts & written notes)
  - electronic files (e.g. electronic records, spreadsheets & emails)
  - conversations (e.g. with patients, family & staff)

Role of the IPC

- The role of the Information and Privacy Commissioner is set out in three statutes:
  - Freedom of Information & Protection of Privacy Act
  - Municipal Freedom of Information & Protection of Privacy Act
  - Personal Health Information Protection Act

- The IPC acts independently of the government to uphold and promote open government and the protection of personal privacy.



Consequences

- Disciplinary action through UHN's Human Resources Department
- Disciplinary action through your regulatory college
- Monetary – fines through IPC or potential lawsuit
- Reputation & loss of public confidence

Privacy Commissioner's Update

New Commissioner Appointed January 2015

Outcome Focus:

- Accountability and Privacy Management Framework
- More prescriptive on missing gaps
  - Robust pro-active and re-active system audits, including technical controls to limit wide open searches for patients
  - Comprehensive annual privacy training and awareness program that tracks completion
  - Demonstrated evidence that individuals accessing electronic systems using PHI are aware of the consequences for contraventions of the Act and your organization's corporate policy
  - Individual and organization accountability – Prosecutions for violations of unauthorized accessed

Past:

- Privacy by Design – Moving forward with build as you go

Changing External Landscape

Key Changing Business and Legislation Drivers

Ontario's Patient First Plan

- Health Links provides coordinated, efficient and effective care to patients with complex needs
- Shared electronic systems to support these activities
- Patients and families engage as Partners in Care

Data as a Strategic Asset

New Healthcare Actors

- Apple, Facebook

PHIPA amendments

Increased Privacy and Security Risk

Legal Suits & Class Actions

Shared Electronic Systems – with shared accountability

- Provincial
- Regional
- LHIN
- Hospitals

PHIPA Legislative Amendments Released In Spring

Increased Security Threats – Cybersecurity

Example: UHN's Privacy Office

VISION

To enable UHN to successfully execute its business models in transforming health care delivery by leading a best-in-class, enterprise-wide privacy program

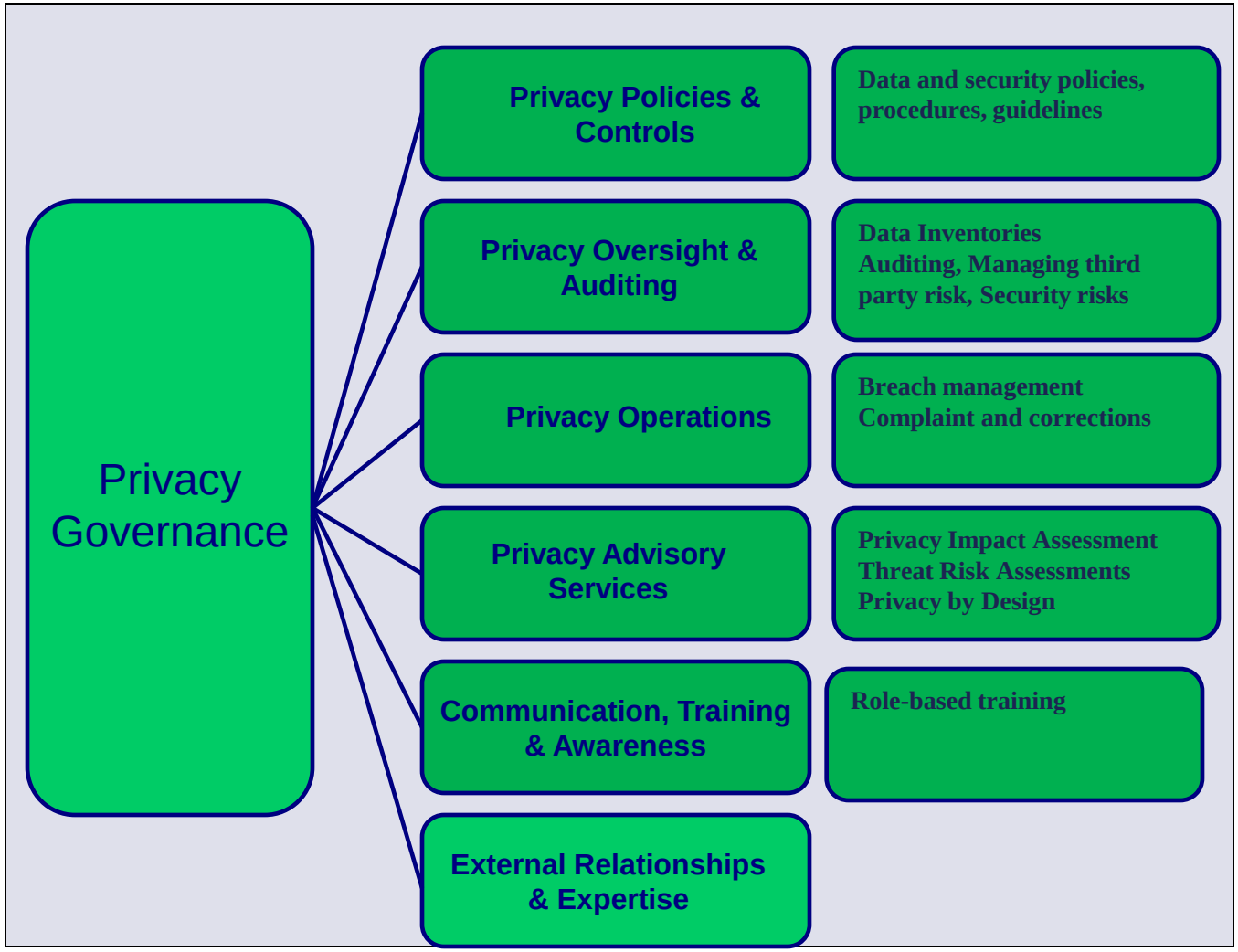
MISSION / PURPOSE

To embed privacy in the foundation and culture of UHN

- The Privacy Office plays a role in:
  - providing legislative oversight, developing corporate policies and monitoring compliance
  - managing privacy breaches/incidents;
  - training staff and providing resource materials
  - helping staff make privacy decisions when ethical dilemmas are not covered in the law or within UHN policies
  - assessing privacy impact of new technology, processes, vendor contracts, etc.
  - responding to patients' privacy concerns and providing education materials

Privacy Management Framework

Privacy strategy and direction for the enterprise, and decisions on key privacy issues.



Example: Accountabilities and Responsibilities – Board members

Boards Accountabilities & Responsibilities

Governance –
- responsible for the overall governance of the HSP
- to ensure that it has put in place adequate oversight and protections (ex. people, processes, policies, protocols) to ensure the hospital's compliance with the privacy legislation.

Non-compliance –
- must track non-compliance and ensure that it is addressed in a timely manner until compliance is achieved.

Liability and Reputational Risk -
- oversees legislative compliance by the board
- to reduce the potential exposure of the hospital to liability (i.e. through lawsuits including class actions)
- PHIPA imports potential for personal liability of Board members (Section 72). Technically, if we were perfectly PHIPA compliant, we would not have much if any risk of liability for privacy breaches. However, this is not currently the reality, and with the evolving litigation landscape and class actions, the Board needs to be aware of and understand what the greatest liability risks for the HSP are so it can make informed decisions about how to allocate resources and best protect the HSP.

Support a culture of privacy

Example: Accountabilities and Responsibilities

Enterprise Privacy & Access Office (EPAO)	Executive & Department Managers	Managers	Employees
• Enterprise governance, framework, strategy • Centre of excellence for privacy advice • Enterprise policies, controls, standards • Training strategy & curriculum • Reporting & escalation to senior leadership • External communications & relationships	• Customize policies for own business • Implement own procedures • Follow EPAO's assessment methodology • Self-identify risks that need monitoring • Work with EPAO to design risk management controls • Coordination & reporting to EPAO	• Understand/ implement relevant policies • Assist with patient complaints • Report & escalate incidents • Ensure staff trained, knowledgeable	• Support privacy investigations & audits • Ensure access controls followed

Support a culture of privacy

Controls – Privacy tools

Privacy Office must haves?

- Personal Information Inventory
- Policies/Procedures/Guidelines/Standards
- Risk Assessment tools
- Training and Education requirements
- Breach and incident management response
- Service Provider Management
- External Communication

Privacy by Design Considerations

How Information Technologists Can help?

- Strong auditing capabilities
- Flexible Patient consent model
- Secure Patients access capabilities – electronically or extractable
- Reminders to keep things confidential – printer tags
- Flexible role access
- Appropriate use controls

Accountability - Knowing your program is working

You need to:

- Identify adequate resources
- Build in privacy protection into every major function involving the use of personal information

Achieve this by:

- Knowing the major functions/process in your organization
- Ensuring transparency
- Being measurable against targets
- Ensuring you have the right tools available

Types of Reporting

Departmental

- Weekly incident report
- Aging of outstanding risks from PIA
- Unresolved complaints
- Result from compliance review
- Monthly incident reports

Compliance/Management

- Non-compliance certificate
- Quarterly breach reporting
- Training

Regulatory

- Regulatory reporting on incidents and access request

Project

- Privacy Impact Assessment
- Un-resourced projects

Board

- Results from Compliance reviews
- Themes from breaches, complaints
- Emerging risks

Changing life of a Healthcare CPO

Function	Current State	Future State = Current plus….
Privacy Policies & Controls	• Organizational policies	• Shared electronic system policies outlining in detail roles and responsibilities
Oversight and Monitoring	• Employee signs organizational confidentially agreement • Ensure notices were up and running • Limited compliance reviews – mostly done through accreditation reviews	• Increased compliance monitoring in departments • Introduction of attestation processes • Multiple end-user agreements for shared systems

Changing life of a Healthcare CPO

Function	Current State	Future State = Current plus
Operations	• Organizational incident management • Audits review completed • Complaint and correction • Access Requests • Consent directives management • Notice	• Increased audits on existing systems and people • New audits from shared systems • Coordinated complaint and correction handling • Additional notification to patients on consent directive • Changed notices
Advisory Services	• Privacy Impact Assessment and Threat Risk Assessments • Contract reviews	• Less impact on whether agree with mitigation plans because run through governance committee • Privacy by Design in technology solutions
Training and Awareness	• One time organizational training	• Refresher training • shared system training – role based and more detailed

What Does Success Look Like?

Silence

- Patients feel their obligations and rights are understood and followed
- Privacy and Security controls are part of the technology solutions
- Employees understand their obligations
- Employees feel comfortable reporting non-compliant events
- Complaints don’t highlight repetitive non-compliance controls
- Breach investigations don’t highlight systemic issues

Lessons Learned

- Align the privacy strategy with company business strategy
- Build privacy and security controls directly into the solutions
- Integrate training and compliance into employee job responsibilities and make
  it part of the annual review
- Watch for emerging trends locally and globally

Appendix

Robin.Gould-Soil@uhn.ca
14-6937

Comments From The Rouge Valley Order

The health information custodian has the onus of establishing compliance with section 12(1) of the Act. While the hospital claims that it has complied with section 12(1), it has not provided me with any information or evidence to support its claims about the practices in place in the Ontario Health sector. Nor has it explained how its safeguards "have been tested" against "the requirements established for regional information technology initiatives: including the Hospital Diagnostic Imaging Repository Services. Nor, has it provided me with any information or evidence about the safeguards used by other Meditech clients, other than it Hosting provided.

"In my view, reactive auditing is inadequate and does not meet the Hospital's obligations pursuant to section 12(1) of the Act and is contrary to the Hospital's own policy."

Privacy policies and procedures on their own however are not sufficient. HIC must also take steps to ensure that agents are aware of and understand their obligations and limitations under the ACT and under privacy policies, practices and procedures that custodians have implemented and that agents are aware of and understand the consequences of failing to comply with these obligations and limitations

Comments From The Rouge Valley Order

12(1) of Act, health information custodians must review from time to time the measures or safeguards that they have implemented to ensure that they continue to be "reasonable in the circumstances".

Comprehensive privacy policies, procedures and practices, as well as comprehensive privacy training, are critical in protecting personal health information from unauthorized use and disclosure and from other contraventions of the Act.

Resources

Getting Privacy Accountability Right with a Privacy Management Program, OPC, BC OIPC, AB OIPC, 2012

http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Health Records, COACH, 2013

http://www.coachorg.com/en/practices/2013-Special-Edition-EMRs.asp

Community Governance Consultation Group (CGCG)

Co-Chairs:

Ron Haines, Vice Chair, Mississauga Halton LHIN

David Lukey, Council Member, Canadian Red Cross (Peel Region)

CONTACT: GovernanceGroup@lhins.on.ca

Reminders

- For your name tags, please **tuck the strings into your name tag** and place it in the box on the registration table.
- Your feedback on this event is important! A survey link will be emailed to you in the next few days
- Contact us at GovernanceGroup@lhins.on.ca

Closing Remarks

Ron Haines
Vice Chair,
Mississauga Halton LHIN Board of Directors

Thank you for attenting tonight‘s session

You can find a copy of this presentation at:

www.mississaugahaltonlhin.on.ca

For Health Service Providers

Governance to Governance