Privacy Management Framework

Where We Want to Be

Goal:
• Ability to demonstrate to your company, that you are compliant with privacy laws
• Ability to demonstrate to a Regulator that your company has an effective, up-to-update program in place in the event of a complaint investigation or audit
• Ensure that privacy-related obligations and risks are properly identified - Privacy by default or Privacy by Design principles.

An effective Program should:
• Identify information management practice weaknesses
• Prove good practices are working
• Demonstrate due diligence
Privacy Program Vision

Where We Want to Be

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
Privacy and Access – Escalation and Governance

Finance & Audit Committee
- Approves investment

CEO

SVP & CIO
- Approves Enterprise Privacy strategy framework, governance and policies, training and ensures it aligns with UHN Strategy
- Oversees Privacy and compliance risk management
- Receives Annual report
- Advances on appropriateness and implementation of policies across enterprise
- Receives Progress reports

Enterprise Privacy and Access Office
- Develops enterprise governance, framework, strategy, policies, controls and standards
- Develops training strategy and curriculum
- Reporting and escalation to senior leadership
- Risk management
- External communications and relationships
- Centre of excellence for privacy advice

UHN Operations Committee
- Advise on appropriateness of Privacy and Security IT Enterprise policies, training content supporting tools
- Receive Progress Reports

UHN QCC Committee
- Oversee Patient impacts resulting from Privacy critical and severe events
- Receives incident reports

UHN Enterprise IT Governance

UHN Exec

SMT
Privacy Program: The Framework

Privacy Governance

Privacy Policies & Controls

Privacy Oversight & Auditing

Privacy Operations

Privacy Advisory Services

Communication, Training & Awareness

External Relationships & Expertise

60 assessments completed this fiscal year - small number of high risks remain from previous years

309 complaints/inquires received over last 11 months - Patient Relations or CPO

43 privacy orientation sessions

Privacy strategy & direction for the enterprise, & decisions on key privacy issues.
## Accountabilities and Responsibilities

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

Support a culture of privacy
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
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
Organization Commitment - Chief Privacy Officer

Roles & Responsibilities

CHIEF PRIVACY OFFICER

Foundations
- Supervisor, Privacy Advisory Services
  - Senior Advisor, Privacy
  - Advisor, Privacy

Other UHN Entities
- Supervisor, Privacy & Access Operations Program
  - Senior Analyst, Privacy & Access Operations
  - Analyst, Privacy & Access Operations
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
## Program Effectiveness Metrics

<table>
<thead>
<tr>
<th>Priority</th>
<th>Objective</th>
<th>Measure</th>
<th>2013-14</th>
<th>2014-15 Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Oversight</td>
<td>Validate that staff and external stakeholders are appropriately accessing patient information</td>
<td>% of inappropriate accesses that were managed within 7 days of detection</td>
<td>N/A</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of inappropriate access that were managed within 7 days of detections</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Patient Inquiries &amp; Complaints</td>
<td>Promote patient-centred care &amp; appropriate complaint resolution and be aware of policies</td>
<td>% of patient complaints resolved within 30 days</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of patient complaints substantiated internally (i.e. UHN found to be non-compliant)</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of patient complaints substantiated by IPC (i.e. UHN found to be non-compliant)</td>
<td>33%</td>
<td>0%</td>
</tr>
</tbody>
</table>
# Program Capacity Metrics

<table>
<thead>
<tr>
<th>Priority</th>
<th>Objective</th>
<th>Measure</th>
<th>2013-14</th>
<th>2014-15 Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Oversight</td>
<td>Implement adequate oversight and auditing functions to enforce privacy policies</td>
<td># and % of targeted proactive/random audit review completed</td>
<td>N/A</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td># and % of business units where policy oversight audits were conducted</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Patient &amp; Staff Inquiries or Complaints</td>
<td>Ensure capacity of Enterprise Privacy Office meets demands of patients</td>
<td># of general inquiries received from staff</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td># of consent directives requests received and # processed</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td># of escalated complaints requests received</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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
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