Making Shared Accountability Work

IAPP Canada Privacy Symposium 2014 – May 8, 2014

Robin Gould-Soil, CPO, ConnectingGTA, University Health Network
Natalie Comeau, Supervisor - Privacy Advisory Services, ConnectingGTA, University Health Network
Agenda

1. What is shared accountability?
2. Governance & roles within the ConnectingGTA Program
3. Technical & business requirements development
4. Examples of designing a privacy & security conscious tools
5. Top 10 lessons learned
What is Shared Accountability?

What is shared accountability?
• Getting to place of mutual acceptance to shared policies, procedures & agreements (e.g. have patient centric practices)

How do we achieve shared accountability?
• Ensure all parties have leeway to fulfill own responsibilities (enabling all parties to meet obligations)
• Focus on areas of high risk
• Identify roles, clearly structure roles together, ensure parties understand their roles & respect other roles

Examples of how accountability is operationalized
• Technical design
• Policies
• Operational practices
• Tool sets
Governance & Roles Within the ConnectingGTA Program
**ConnectingGTA – Year in Review**

**Adoption**

175+ Clinicians directly involved
- Clinician Champions previewed solution to support LPR
- Kicked-off Benefits Evaluation work stream and engaged stakeholders to help prioritize key indicators
- Sites submitted initial user estimates to reach ~34,000 end users

**Implementation**

15 Early Adopter organizations populating the CDR since May 2013
- Early Adopter sites have connected to the ConnectingGTA Provider Portal and completed ConnectingGTA federation and access validation
- Early Adopter Sites confirmed acceptance and compliance of the ConnectingGTA Privacy & Security policies

**Solution Delivery**

~90% of standards-based technical solution built and connections established with provincial assets (OLIS)

~24 million messages captured in the CDR
- Established end-to-end Portal connections with the HIAL and the associated Provider and Client registries in our development environment
ConnectingGTA – Year in Review (cont.)

- Created Privacy & Security policies; leveraged as foundation for eHealth Ontario’s provincial policies
- Privacy & Security Committee established
- Published LPR Privacy & Security Manual and tools for HICs
- Built in privacy & security business requirements in the design and architecture of the solution to support a shared electronic system
- Developed a privacy management framework that ensures compliance with PHIPA and supports MOHLTC policies to become regulation

~2.15 million patients captured
- Planning underway with MOHLTC to integrate with the Ontario Drug Benefit database
- Established connection and feed to Hospital Report Manager
- Completed Wave 2 (Expansion) site selection and initiated planning
Privacy and Security Framework

Governance Committees

Steering Committee
Privacy and Security Committee
Privacy and Security Working Group

Makes decisions about and guides

Planning of Program
Advising
Monitoring and Reporting
Assurance

Privacy and Security Policies, Procedures, and Practices

Defines and guides

Access and Correction
Privacy Logging and Auditing
Inquiries and Complaints
Privacy Breach Management
Consent Management
Security Logging and Monitoring
Information Systems Development
Information and Asset Management
Business Continuity
Cryptography
Physical Security
Network and Operations
Access Control and Identity Management
Security Incident Management

Activities to manage the privacy program

Activities to meet the privacy and security operational obligations

People

Communications
Training
Support
Management

Technology

Privacy and Security
Framework
Privacy and Security Key Deliverables

- Business Requirements
- Privacy, Security and Federation readiness assessments
- PIAs and TRAs, including managing RTPs
- Training strategy and content
- Agreement provisions
- Manuals for HICs and HINP
  - Implementation Guides
  - Tools to support policies
- Risk framework and policy exception process
ConnectingGTA Program Governance Structure

**Program Steering Committee**
- Clinical Working Group
- Technical Working Group
- Privacy & Security Working Group

**ConnectingGTA Program Team**

**Participating Organizations & Clinical Systems**

**FUNDERS**
- eHealth Ontario
- Canada Health Infoway

**KEY INFLUENCERS**
- Central Ontario Electronic Health System Council

39 individuals representing six ConnectingGTA LHINs and clinical perspectives across the care continuum:
- CCACs
- Complex Continuing Care
- Family Physicians
- Hospitals
- Mental Health & Addictions
- Nursing
- Pharmacy
- Rehabilitation
Privacy & Security Governance Structure

Privacy and Security Committee (PSC) – operational oversight

Privacy and Security Working Group (PSWG) - design and development of technology, business practices & privacy & security program

Privacy & Security Team (PST) - supports the PSWG and PSC, perform the day-to-day operations of the privacy and security program
Structuring the Privacy & Security Team (PST)

Business analyst skills – writing business skills, building test plans, scenarios, quality control

Privacy analyst skills

Security analyst skills

Policy and procedure development

Communication skills – notices, websites

Security architectural skills

Understands business & clinical needs

Operations

Program & project management skills, governance

Relationship management
Structuring the Privacy & Security Working Group (PSWG) & Privacy & Security Committee (PSC)

Select CPOs from participating sites

Select CPOs from GTA healthcare organizations

eHealth Ontario (rep)

Information & Privacy Commissioner of Ontario (rep)

Canada Health Infoway (rep)

ConnectingGTA privacy & security leads

eHealth Ontario (as data source contributor)

CISOs from participating sites (half of site reps)

CPOs from participating sites (half of site reps)

PSWG

PSC
Participating HIC Responsibilities

Detailed operational responsibilities outlined in Privacy and Security Manual

- Report & respond to security incidents & privacy breaches
- Ensure consent is obtained
- Register consent directives or forward to ConnectingGTA
- Review consent directive overrides and inform the patient/client
- Answer questions and complaints
- Conduct audits
- Provide patients/clients with access to his or her PHI or an audit of access
- Ensuring correction to PHI requests are addressed
- Enable logging & monitoring capabilities on local systems
- Ensure access and identity management controls are in place to manage all person and system access to ConnectingGTA
## Examples of Centralized & De-centralized Functions

<table>
<thead>
<tr>
<th>Policy</th>
<th>Centralized – ConnectingGTA Program Responsibilities</th>
<th>De-centralized – Site Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access and Correction</strong></td>
<td>• ConnectingGTA will receive &amp; respond to requests from patients/clients</td>
<td>• Address the inquiry or complaint, or forward to ConnectingGTA</td>
</tr>
<tr>
<td><strong>Consent Management</strong></td>
<td>• Assist HICs in creating, modifying, or deleting consent directives</td>
<td>• Create, modify, or delete consent directives received</td>
</tr>
<tr>
<td></td>
<td>• Ensure HICs are notified of consent directive overrides</td>
<td>• Review consent directives overrides</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Notify the patient of consent directive overrides</td>
</tr>
<tr>
<td><strong>Logging &amp; Auditing</strong></td>
<td>• Log all activities</td>
<td>• Audit their agents and electronic service providers</td>
</tr>
<tr>
<td></td>
<td>• Make reports of activities available to HICs</td>
<td></td>
</tr>
<tr>
<td><strong>Training</strong></td>
<td>• Provide and refresh training materials</td>
<td>• Ensure that agents are informed of their obligations before using the system</td>
</tr>
</tbody>
</table>
Lessons Learned – Governance

Top 5 things that worked well:

1. Clearly setting & managing expectations
2. Tracking decisions, changes and successes
3. Embedding dedicated privacy resources into all program aspects (e.g. having privacy specialists participate in the Clinical Working Group system design sessions ensured privacy was built into non-privacy functionality)

And because every decision can’t go back to the committee:

4. Building rules about when need to engage committee (e.g. summary policies, what needs to come to committee, how decisions by other committees will be communicated)
5. Deciding when to consult committee as a group and when to consult individual committee members
Lessons Learned – Governance

Top 5 things that we would change:

1. Ensure cross-representation from the start (e.g. Clinical Working Group member at the Privacy & Security Working Group)
2. Ensure better security representation on Privacy and Security Committee from the start
3. Co-chair the Privacy and Security Committee with someone who is not part of the program team
4. Provide opportunities for discussions without the regulator at the table
5. Provide sufficient time to review documents (and not in the summer) & ability to review others’ comments (e.g. via shared drives, teleconferences)
Technical & Business Requirements Development
Requirements Development Process

- Clinical committee developed Business Requirements Document (BRD)
- Three working groups vetted and added to BRD
  - Clinical Working Group
  - Technical Working Group
  - Privacy & Security Working Group
- BRD translated into RFP
- After vendor selected, three working groups continued to develop requirements, considering resource constraints
  - Additional groups: Clinical Solution Team and Program Clinical Team to review product from vendor & recommend changes to Front-End Provider Portal
- Final decisions reviewed with all working groups, based on acceptance criteria and demonstrations of functionality

Privacy by Design Principles

Proactive not Reactive – Preventative not Remedial

Privacy as the Default Setting

Visibility & Transparency – Keep it Open
Iterative Design Process for Policies

- Highly engaged groups
- Requirements circled between Privacy & Security Working Group (including representation from eHealth Ontario) and participating sites
- Approved by Privacy and Security Committee & Steering Committee
Iterative Design Process for Technical Functionality

- Highly engaged groups
- Requirements circled between vendor, Clinical Working Group and Privacy & Security Working Group/program privacy and security specialists
Examples of Designing a Privacy & Security Conscious Tools
Implementing a Robust, Patient-Centered Consent Model

Types of Consent Directives:
1. Global
2. (Domain)
3. HIC-Records
4. HIC-Agents
   - One agent
   - All agents
## Implementing a Robust, Patient-Centered Consent Model (Continued)

<table>
<thead>
<tr>
<th>Clinical / Business Need</th>
<th>RFP</th>
<th>Technical Capability</th>
<th>PSWG</th>
<th>Final Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patients must be able to ‘opt out’ of PHI sharing at many levels</td>
<td>• Support 6 levels of consent directives</td>
<td>Consent Management Tool (HIPAAT Privacy eSuite) used for consent management by CPOs and Front-End Provider Portal</td>
<td>5 levels of directives supported</td>
<td>Robust consent management process in the back end</td>
</tr>
<tr>
<td>Clinical end users need to be able to apply consent directives &amp; override consent directives easily where appropriate</td>
<td>• Limit display of PHI subject to a directive</td>
<td>* Additional input from IPC, Ministry of Health and Long-Term Care, eHealth Ontario</td>
<td>3 click override process for clinicians</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Honor directives from other domains</td>
<td>Consent directives are flexible to manage and can evolve as technology adoption evolves</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lessons Learned - Consent Model

• Clarify principles & goals (e.g. patient-centric process)
• Technical component easiest; change management is more challenging
  • Organizations’ models
  • Patients’ expectations
• Anticipate changes – procured flexible electronic tool
• Gave sites tools to review operational impacts & provide feedback (including how departments and business units across an organization are affected, such as Health Records)
• Iterations of functionality for CPOs
• Need to leave time/processes to consider feedback from usability testing & incorporate where appropriate
# Designing a Comprehensive & Secure Patient Search

<table>
<thead>
<tr>
<th>Clinical / Business Need</th>
<th>RFP</th>
<th>Technical Capability</th>
<th>PSWG</th>
<th>Final Functionality</th>
</tr>
</thead>
</table>
| Find the right patient | Solution should support searching with unique ID, MRN, OHIP, name, date of birth, gender | Possible:  
- different combinations of fields  
- some or all fields mandatory | ✓ Include enough PHI for positive identification  
✓ Use no more PHI than necessary  
✓ Only return 1 patient whenever possible | Clinicians can do 1 of 3 searches:  
1. OHIP & name & gender  
2. MRN & org name  
3. Advanced Search (any of name, DOB, gender, address) |
| Find a patient with a unique # (OHIP or MRN) | | | | No information displayed if more than 5 results match |
| Find a patient in an emergency (no unique #) | | | | |
Lessons Learned - Designing Patient Search

• Other shared systems (e.g. PRO) that require a match of 3 identifiers, including OHIP and DOB, prevent ‘fishing trips’ but do not work in outlying scenarios, such as emergencies
• eHealth Ontario requirements were added after RFP during design phase
• Patience! Design phase took 3 cycles of iteration between Privacy and Security Working Group, Clinical Working Group and vendor
• Considerations:
  • Variety of clinical scenarios reviewed/tested (e.g. emergency)
  • Limiting results to reduce PHI ‘leak’/exposure (contact info or fact that person was a patient at a particular institution)
Enable fast & coordinated responses to breaches by clearly defining & articulating the roles of multiple parties

Defined privacy incidents (breaches)
Required HICs & HINPs to work together at each stage of incident management
Required identification of an Incident Lead to coordinate responses & reports

Technical: logging & auditing capabilities

RACI

✓ All breaches involving ConnectingGTA must be reported
✓ All impacted HICs will be notified
✓ Most responsible party does task
✓ Breach Investigator chosen to coordinate & report
✓ HICs will choose which one will notify patients
✓ ConnectingGTA will report to PSC & SC

Responses are coordinated, whether:
• Caused by a HIC & related only to that HIC’s PHI
• Caused by a HIC & related to other HICs’ PHI
• Caused by multiple HICs
• Caused by ConnectingGTA or an unauthorized party
### Ensuring Parties can Respond Quickly to Privacy Breaches (Continued)

#### RACI for Privacy Breach Management
- Depicts who is responsible, accountable, consulted, and informed

E.g. A HIC is responsible for a breach affecting PHI contributed by another HIC:

<table>
<thead>
<tr>
<th>Action</th>
<th>HIC(s) that caused</th>
<th>HIC(s) that contributed PHI</th>
<th>Breach Investigator</th>
<th>Containment Lead</th>
<th>Privacy Operations</th>
<th>cGTA P&amp;S Lead</th>
<th>cGTA Senior Leads</th>
<th>Other cCGTA Team Members (as required)</th>
<th>PSC/SC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Notification</td>
<td>R</td>
<td>I</td>
<td>N/A</td>
<td>N/A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Containing the Breach</td>
<td>C,I</td>
<td>C,I</td>
<td>N/A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Investigating the Breach</td>
<td>C,I</td>
<td>C,I</td>
<td>R</td>
<td>N/A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Remediating the Breach</td>
<td>R,I</td>
<td>R,I</td>
<td>N/A</td>
<td>N/A</td>
<td>R,I</td>
<td>I</td>
<td>I</td>
<td>R,I</td>
<td>I,A</td>
</tr>
<tr>
<td>Notifying Patients</td>
<td>R,I</td>
<td>R,I</td>
<td>N/A</td>
<td>N/A</td>
<td>I</td>
<td>I</td>
<td>N/A</td>
<td>N/A</td>
<td>I</td>
</tr>
<tr>
<td>Notifying IPC, Law Enforcement, &amp; Regulatory</td>
<td>R</td>
<td>I</td>
<td>N/A</td>
<td>N/A</td>
<td>I</td>
<td>I</td>
<td>N/A</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Breach-related Comms</td>
<td>R,C</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>R,C</td>
<td>A</td>
<td>I</td>
<td>C,I</td>
<td>I</td>
</tr>
</tbody>
</table>
Lessons Learned – Breach Management Policy

- Too big to build all at once!
- Establish objectives for policies (e.g. patient and clinician-focused)
- Establish standards for policy writing (e.g. common terminology, format & content)
- Stop and pause to ensure policies and system solution are aligned
- Don’t underestimate the power of good documentation
- Evolve policies into procedures, operating practices and easy-to-use tools

Privacy by Design Principle (#6)

Visibility & Transparency – Keep it Open
Future Challenges

1. Harmonization of policies & procedures
2. Patient awareness, requests & involvement in care
3. Increased users & uses of data
4. Cyber threats
5. Evolution of the program – i.e. governance model, stakeholder engagement, etc.
Thank you!
Questions?