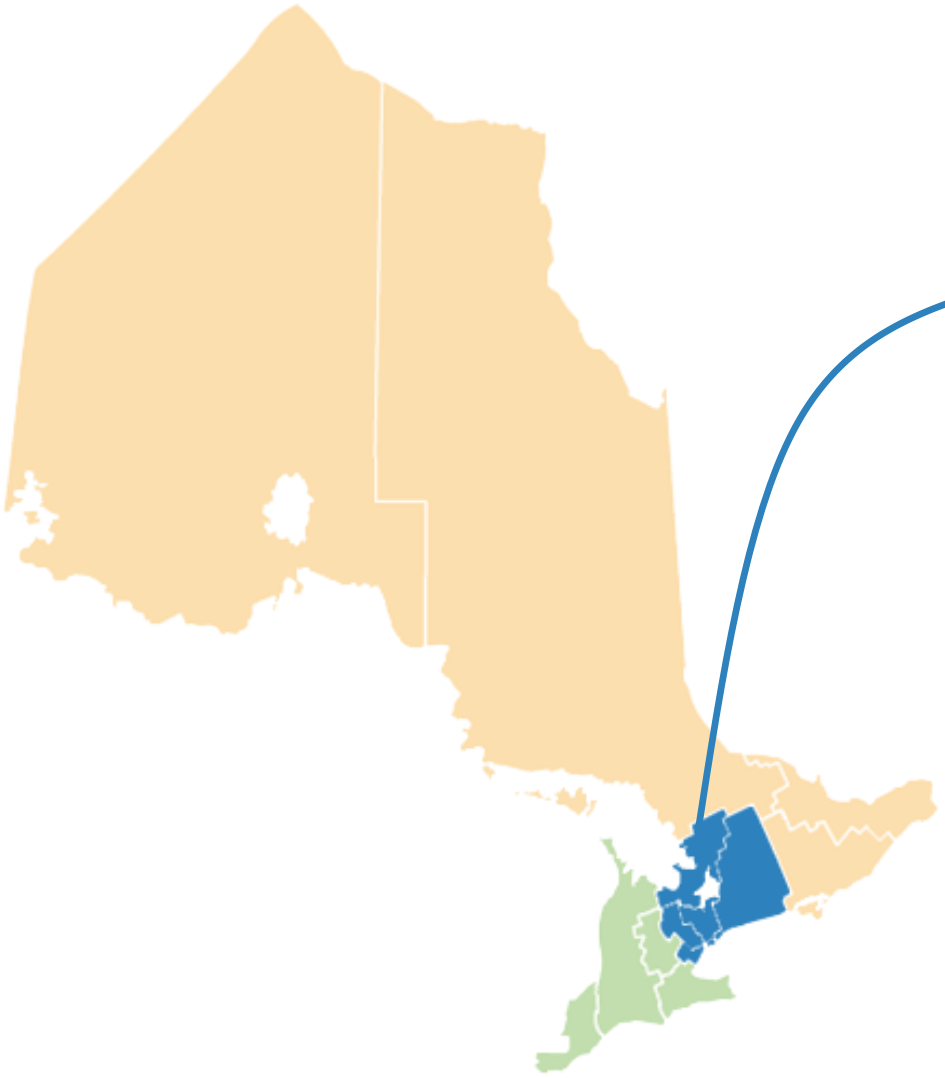
Sharing Privacy: Developing Policy for Shared Systems Environments

eHealth 2015 – June 3, 2015

Robin Gould-Soil, CPO, ConnectingGTA, University Health Network

Natalie Comeau, Supervisor, Privacy Advisory Services, University Health Network

ConnectingGTA is delivering a **regional electronic health record** that will make patient information available at the point-of-care to improve the patient and clinician experience



6 Local Health Integration Networks

750+ Health Care Organizations

6,267 Family Physicians

6,930 Physician Specialists

49,905 Nurses

All sectors of care:

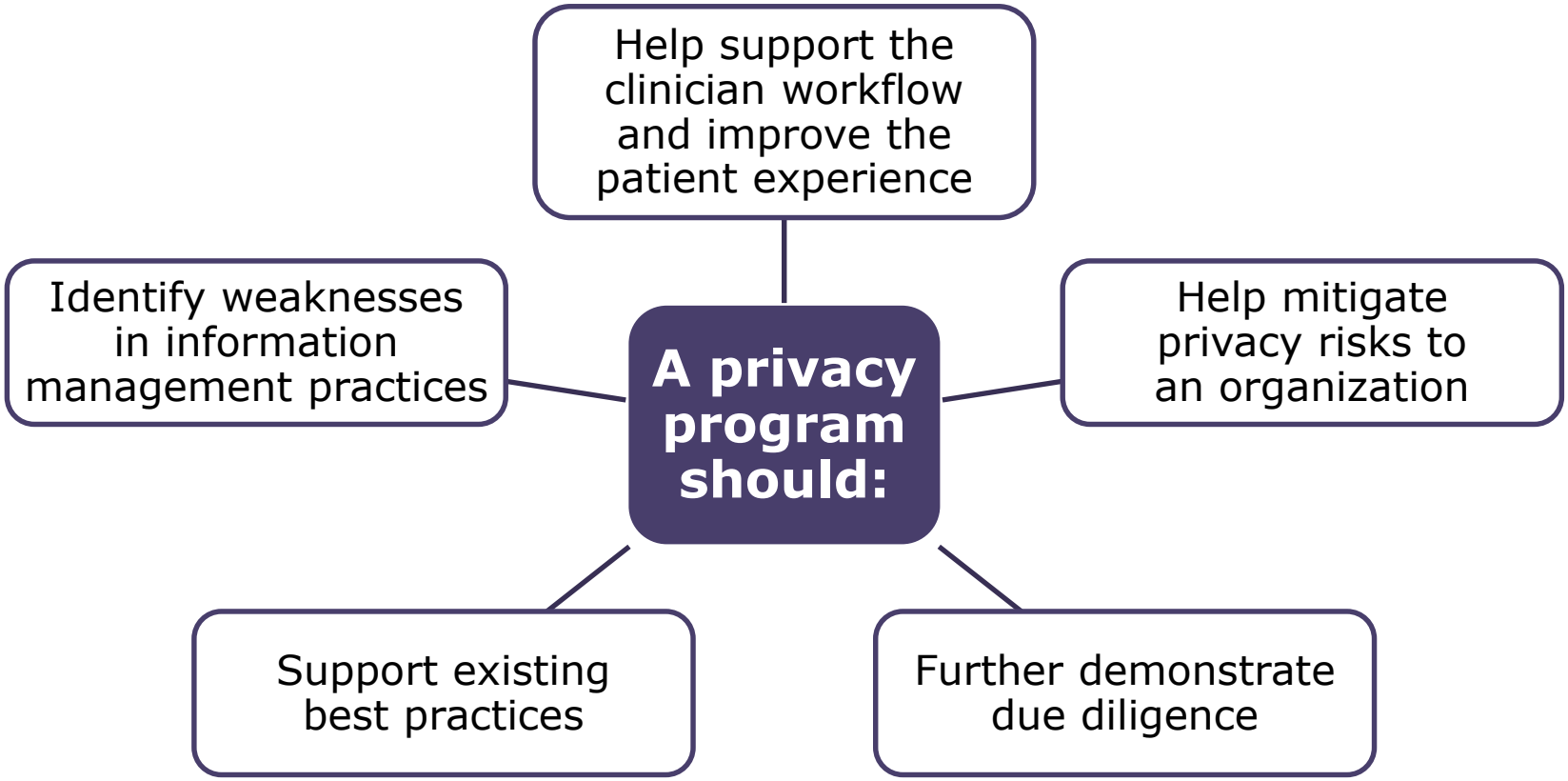
- Acute Care
- Community Support Services
- Complex Continuing Care
- Long Term Care
- Mental Health & Addictions
- Primary Care
- Rehabilitation

Where We Are and Where We Are Going

	Early Adopters	Expansion
Data Available (Hospitals and CCAC data - based on IP Admissions & ED visits in GTA)	**~50%** Acute Data **100%** CCAC Data **~75%** Lab Results	**~80%** Acute Data **100%** CCAC Data **75%+** Lab Results
Clinical Users	**30,000+**	**40,000+**
Number of organizations to benefit	**~40 HSPs**	**~100 HSPs**

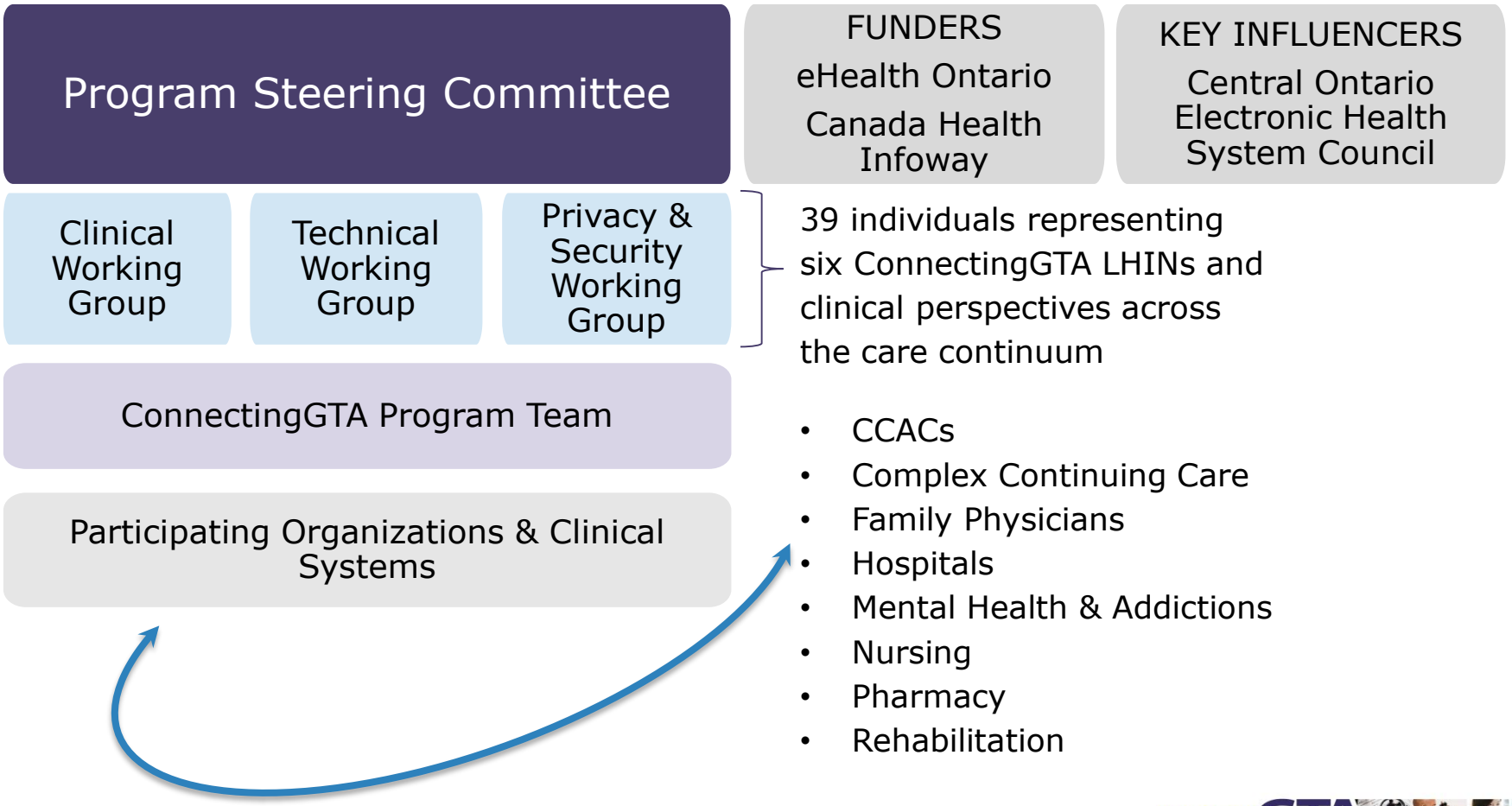
Privacy Management Framework

Where We Want to Be

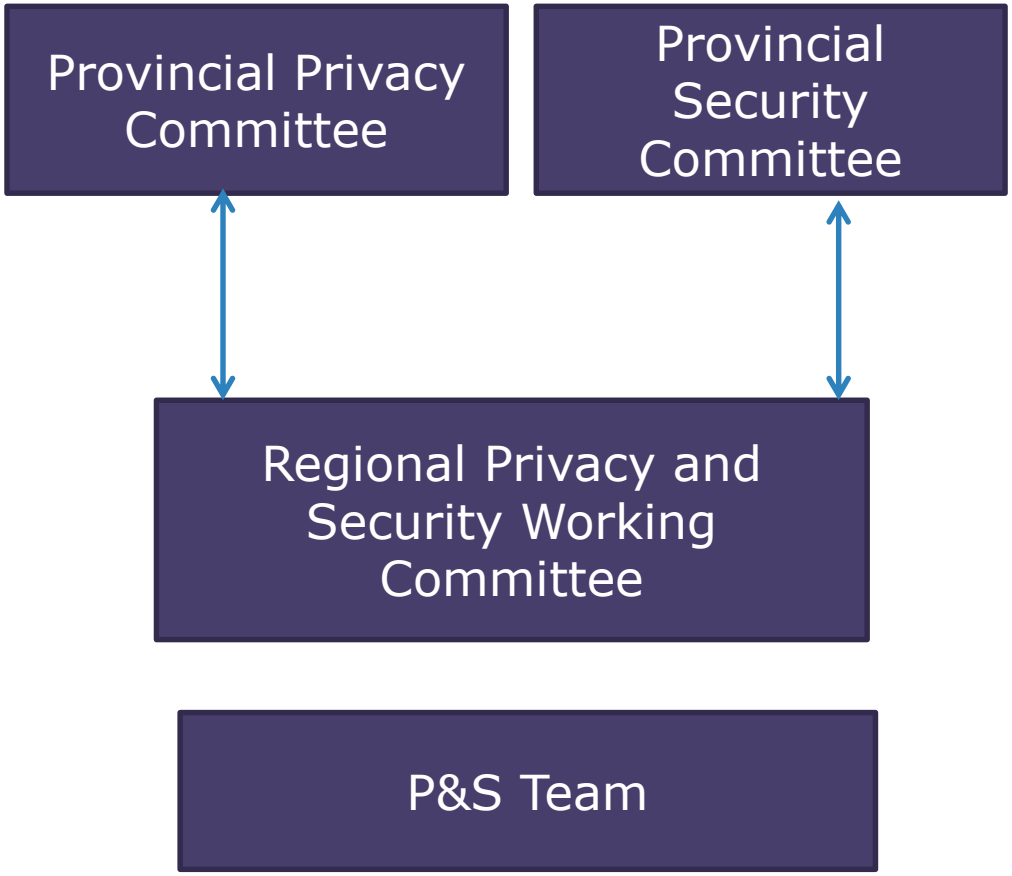


ConnectingGTA Governance Structure

Through collaboration, partnership, strong leadership as well as executive, business and clinical support across six Local Health Integration Networks, ConnectingGTA will deliver the best solutions for its stakeholders



Provincial View – Governance is still evolving



The Regional Privacy and Security Committee (PSC) is responsible advising on design and development, provides ongoing counsel and advice regarding developing of the program as well as provide guidance operational oversight of privacy and security, and reports directly to the ConnectingGTA Steering Committee.

Regional P&S Working committee and are responsible for supporting the day-to-day operations of ConnectingGTA's programs

Privacy and Security Key Deliverables

- Policies
- 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

Introduction to Policies

Policy Structure

Table of Contents

- Purpose
- Definitions
- Scope
- Policies and Procedures
  - Guiding Principles
  - Procedures
- Enforcement
- References
- Document Management
  - Policy Number
  - Version
  - Version History
  - Effective Date
  - Last Review Date
  - Next Review Date

Privacy Policies

- Privacy Policy (TBC)
- Access and Correction
- Consent Management
- Auditing and Logging
- Retention
- Inquiries and Complaints
- Privacy and Security Training
- Privacy Breach Management
- Assuance

Security Policies

- Information Security Policy
- Acceptable Use of Information and Information Technology
- Threat Risk Management
- Cryptography
- Data and Asset Management
- Access Control and Identify Management
- Network and Operations Security
- Information System Development Lifecycle
- Electronic Service Providers
- Physical Security
- Logging and Monitoring
- Incident Management
- Business Continuity

Summary of Privacy and Security Responsibilities and Obligations

Policy	Centralized – ConnectingGTA Program Responsibilities	De-centralized – Site Responsibilities
Inquiries and Complaints, Access and Correction	• ConnectingGTA will receive requests or issues directly from patients as required • ConnectingGTA will forward the issue or request to the relevant HIC if it relates just to one HIC • ConnectingGTA will respond or coordinate the response to issues or requests relating to ConnectingGTA or multiple HICs	• address the request, issue, etc if it relates to that HIC alone; if not the HIC asks the person to contact ConnectingGTA
Consent Management	• create, modify, or apply any consent directives it receives unless the request is to block access to PHI from another HIC as requested by smaller HIC's or patients • notify the HIC in the event of a consent directive override	• HICs should create, modify, or apply any consent directives it receives unless the request is to block access to PHI from another HIC • HICs must review all consent directives overrides and notify the patient
Privacy Breach Management	• Manage Privacy Breaches impacting multiple sites • implement remediation activities as a result of the investigation	• All suspected or real Privacy Breaches must be reported, but only Privacy Breaches impacting multiple HICs will be centrally managed • An appropriate HIC(s) will be chosen to notify patients and investigate breaches that are centrally managed • implement remediation activities as a result of the investigation

Summary of Privacy and security Responsibilities

Policy	Centralized – ConnectingGTA Program Responsibilities	De-centralized – Site Responsibilities
Logging and Auditing	• ConnectingGTA logs everything and will make reports available to HICs to conduct audits required by PSC • ConnectingGTA must both audit their own agents and electronic service providers according to PSC criteria • ConnectingGTA will monitor activity of HICs' agents and inform the HIC of suspicious activity	• HICs must audit their own agents and electronic service providers according to PSC criteria • May eonduct audits for HIC's that they are sponsoring the solution too.
Privacy and Security Training	• ConnectingGTA will provide and refresh training materials • Manage the end-user agreements within the system	• HICs and ConnectingGTA must provide ensure that their agents are informed of their relevant obligations and receive training before using the system
Assurance (in draft)	• ConnectingGTA will conduct PIAs/TRAs (various triggers), and self-attestations every year and risk treatment plans • ConnectingGTA will remediate high and risk risks • ConnectingGTA may be subject to audits • Prepare Information Notices •	• HICs will complete self-assessments prior to participation and self-attestations every year thereafter • HICs will remediate high risks • HICs may be subject to audits • Ensure Information notices are updated to included that they participate in shared electronic systems

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

12

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	• PIA and TRA's • 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

13

Supports Available to Ease Policy Implementation

- Policies part of a broader toolkit and set of activities to support HICs

- Other supports include:
  - Privacy and Security Manual with step-by-step guides and diagrams on the procedures
  - Training materials
  - Sample templates (e.g., Notice of Purposes)
  - Ongoing access to the ConnectingGTA support line
  - ConnectingGTA executing some business processes on behalf of the HICs
  - Quick Reference guides
  - Quick summaries
  - Webinair

Lessons Learned

Lessons learned

Top Three things that worked well

- Policy Development – patient and clinician focus; established standards
- Governance – set and managed expectations; tracked success
- Designated person to consolidate feedback and work offline to ensure comments were effectively addressed

Results - Sites feel confident that they can comply with privacy obligations and majority of the security obligations ; and have sufficient time to comply with the additional operational obligations

Top 3 things we'd change – purpose and what we'd change

- Better security representation on Privacy and Security Committee
- Must have co-chair that is not someone who is part of the solution
- Sufficient time to review documents – both committee members and participants
- Need a few session without the regulator at the table
- Stop and pause to ensure policies and system solution are aligned
- Test and Learn

Top Lessons Learned

- No two organizations are the same
- Be prepared to change
- Agree on common terminology
- Separate the policy from the standards
- Align participant's privacy programs

Thank You!

Robin Gould-Soil, CPO
Robin.gould-soil@uhn.ca
416-340-4800 ext. 6620

Natalie Comeau, Supervisor, Privacy Advisory Services
Natalie.comeau@uhn.ca
647-539-4636