Privacy & Security for Access Control

Information Governance Summit 2017

Dr Douglas Kingsford
CMIO, Interior Health Authority
Co-chair Information Privacy & Security Standing Committee
IMITSC, HISSC, JCC IM/IT CAWG, Canada Health Infoway DHASC

Privacy & Security Issues

Evolving Operational Context

Coming soon:

- Primary Care Networks
- Community, HA, FN staff working in one another's clinics, closely collaborating in patient care
- Virtual care interactions with multidisciplinary teams – community and HA providers, distributed data
- Mash-ups: views into data from disparate systems – users are community/HA/PH providers, patients
- Loose coupling of systems subject to PIPA, FIPPA, eHealth Act, Pharmaceutical Services Act
- Core provincial infrastructure including eHealth repositories (identity registries)
- Need for secondary use capability at local, regional and provincial levels; need to link datasets for operations research

Privacy & Security Issues

Pressing Issues

- Interactions between HA’s/MoH, community providers
- Interactions with FNHA clinics/providers (same issues?)
- Harmonization of authentication & access models
- Consistent role-based security & access model that can evolve to be under patient control
- Network, applications defense in depth
- Data governance model for secondary use
- Governance in general
- … and more

Relevant Legislation

- FIPPA (Freedom of Information and Protection of Privacy Act)
  - applies to public bodies, professional bodies, etc
  - applies to custody *or control*
  - based on prescribed authorities and notification, not consent
  - concept of “consistent purpose”
  - storage *and access* must be in Canada

- PIPA (Personal Information Protection Act)
  - applies to everyone else (some exclusions apply)
  - based on implied consent, opt-out, limitations of consent

- Access to Information Act, Privacy Act, Personal Information Protection and Electronic Documents Act (PIPEDA)
  - applies to federal institutions and interprovincial information sharing unless other Acts apply

Relevant Legislation

- eHealth (Personal Health Information Access and Protection of Privacy) Act

  - applies to certain designated "health information banks"
  - PLIS, client registry, provider registry
  - covered by "designation orders" – what is collected, why, who can access, any other conditions
  - notion of "disclosure directive" – patient restricting access

- Pharmaceutical Services Act

  - PharmaNet access rules

- Public Health Act

  - Panorama
  - addresses Medical Officers of Health reporting communicable diseases, etc

- Ministry of Health Act, Medicare Protection Act, etc

Key Issues

- Need legal authority – to collect, use or disclose.
- ISA does not in itself establish legal authorities – it only sets out rules for privacy compliance when the legal authorities already exist.
- Distinction between primary and secondary use.
- Different rules apply to data from different sources.
- Unclear if able to share data between PIPA and FIPPA organizations for QI & planning.
- Regional variation:
  - in privacy & security policies
  - in interpretation on what can and can't be shared with whom, with or without consent
  - in expectations when completing PIAs or STRAs on how certain risks are assessed
- Decentralized, uncoordinated data governance.

PRIME

(PharmaNet Revisions for Information Management Enhancements)

- Currently under development.
- Introduces a single, standardized, centralized process for granting, managing, monitoring access to PharmaNet.
- Pharmaceutical Services Act makes MOH the single point of accountability for access to PharmaNet.
- Specific requirements follow from legislation.

GHISA
(General Health Information Sharing Agreement)

- Common framework for information sharing between health authorities, Ministry of Health and certain other providers.
  (in place since March, 2016)

- Directly covers MOH, VPP, FHA, IHA, NHA, VIHA.
  Indirectly covers physicians, PHC, private labs, Excelleris;
  FNHA not mentioned

- Covers physicians delivering services on behalf of HA, others must sign ISA containing applicable GHISA terms; affiliated organizations can agree to be bound by applicable terms in GHISA.

- Relies on Common Access Management Framework, information security policies, procedures for handling data for secondary use.

- Automatically applies, so no need for separate ISA.
  ISPs replace ISAs where data exchanged for 2^{o} use.

- Still need PIA to establish privacy & security protocols.

COIPA
(Common or Integrated Program Agreement)

- Agreement under FIPPA that enables information sharing across a distributed team incorporating public and private providers, particularly with regard to secondary use for planning & evaluation.

- Clarifies legal authorities, standard information sharing rules for privacy compliance, consent and notification requirements.

- Currently under development to support PCN model.

- Does not resolve challenges around connectivity between community and health authority IT systems
  - mash-ups of multiple systems, HA staff charting in private EMRs, security requirements around accessing connected systems, etc

- Does not address regulatory implications for health professionals participating in a PCN.

Future

- Sector-wide work on Security & Access models
  - Enhanced security, defense in depth.
  - Enhanced proactive response to emerging threats.

- “GHISA 2” likely
  - A proposal to extend GHISA framework to cover PIPA organizations, universities, PCNs, FNHA, public health initiatives, R&D, etc.
  - Would harmonize relevant IMIS & privacy policies and standards.

- HIMA (Health Information Management Act)
  - Harmonize the various Acts covering health info into one Act.
  - Common rules, policies, protocols.
  - A longer-term option (likely several years to complete).

→ Questions