Privacy Horizon

Implementing Privacy by Design

MEDTECH 2016

NiHi CANADA

National Institutes of Health Informatics

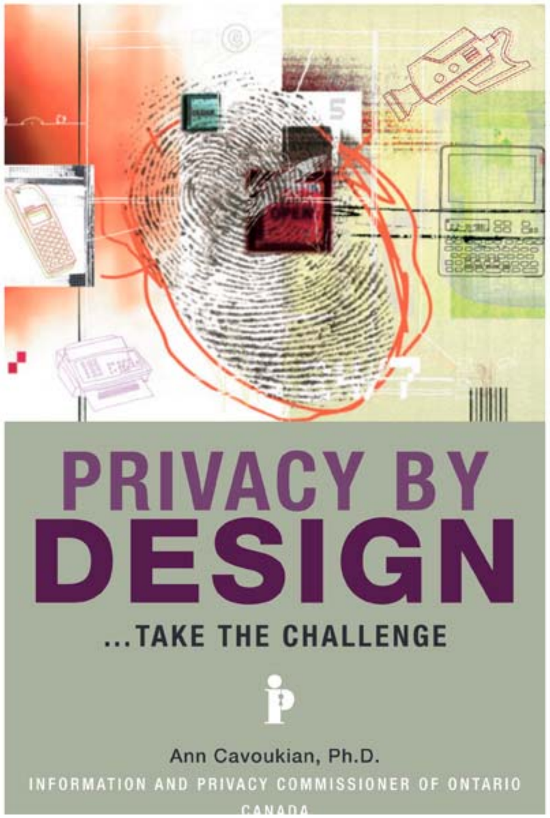
Overview

- Privacy by Design Principles
- Building Privacy into your eHealth Project
- Defining Privacy Requirements
- Being Reasonable – Assessing Privacy Risk

What is Privacy by Design?

- Privacy by Design (PbD) refers to the philosophy and approach of embedding privacy into the design specifications of various technologies.
- PbD can be applied to technology, business practices and physical design.
- Builds privacy into products and services

Privacy by Design



PRIVACY BY DESIGN

...TAKE THE CHALLENGE

Ann Cavoukian, Ph.D.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

CANADA

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

7 Foundational Principles of PbD

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into design
4. Full Functionality – Positive-Sum, to Zero-Sum
5. End-to-end Security – Full Lifecycle Protection
6. Visibility and Transparency- Keep it Open
7. Respect for User Privacy – Keep it User-Centric

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

1. PbD is ***Proactive*** not Reactive; ***Preventative*** not Remedial

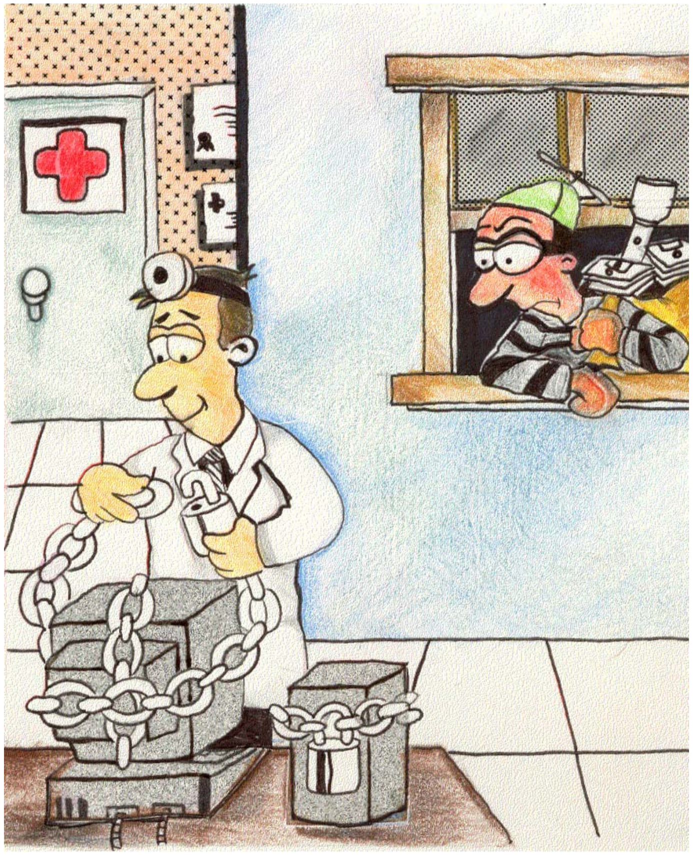
- □ It anticipates and prevents privacy-invasive events before they happen.
- □ *PbD* does not wait for privacy risks to materialize
- □ *PbD* comes before-the-fact, not after.

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

2. Privacy as the ***Default Setting***

- PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.
- If an individual does nothing, their privacy still remains intact.



NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

3. Privacy ***Embedded*** into Design

- Privacy is embedded into the design and architecture of IT systems and business practices.
- It becomes an essential component of the core functionality being delivered.

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

4. Full Functionality – ***Positive-Sum***, not Zero-Sum

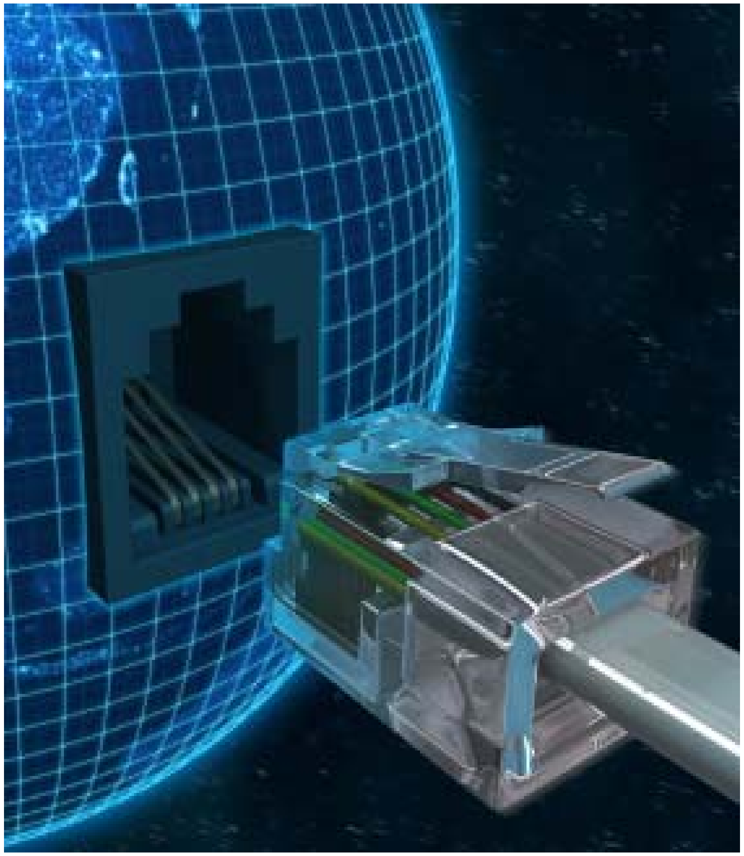
- *PbD* accommodates all legitimate interests and objectives in a positive-sum “win-win” manner.
- *PbD* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

5. End-to-End Security – ***Full Lifecycle Protection***

- *PbD* extends throughout the entire lifecycle of the data involved, from start to finish.
- This ensures that at the end of the process, all data are securely destroyed, in a timely fashion.
- *PbD* ensures cradle to grave, lifecycle management of information, end-to-end.



6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

- Whatever the business practice or technology involved, it must operate according to the stated promises and objectives, and is subject to independent verification.
- Its component parts and operations remain visible and transparent, to users and providers alike. Trust but verify.

7. ***Respect*** for User Privacy – Keep it ***User-Centric***

- *PbD* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Building Privacy Into Your eHealth System

- The privacy ecosystem
- Requirements definition
- Privacy and security architecture
- The PIA and TRA as PbD tools

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

The Privacy Ecosystem

- The Privacy Ecosystem encompasses:
  - People
  - Processes
  - Technology
  - Information

The Privacy Ecosystem

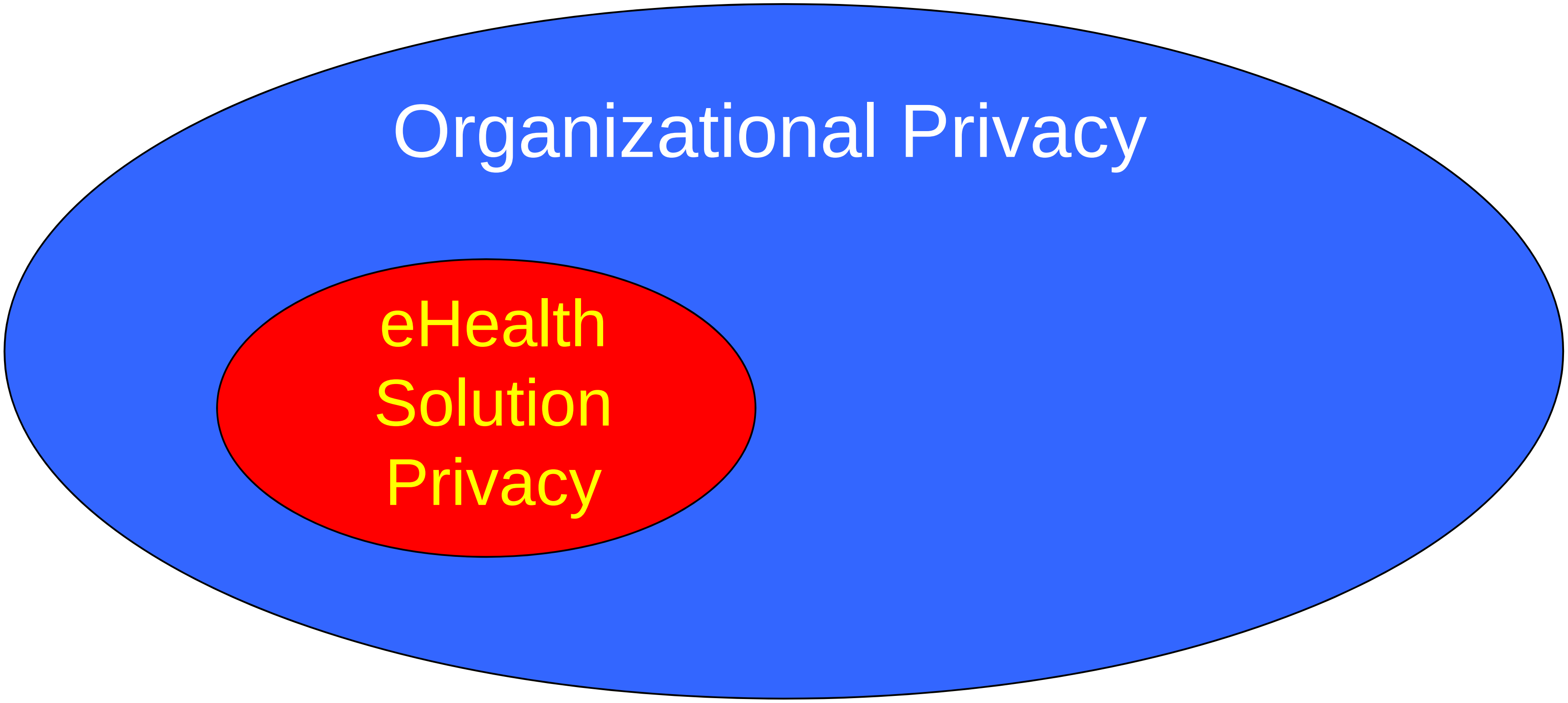
Organizational Privacy

The Privacy Ecosystem

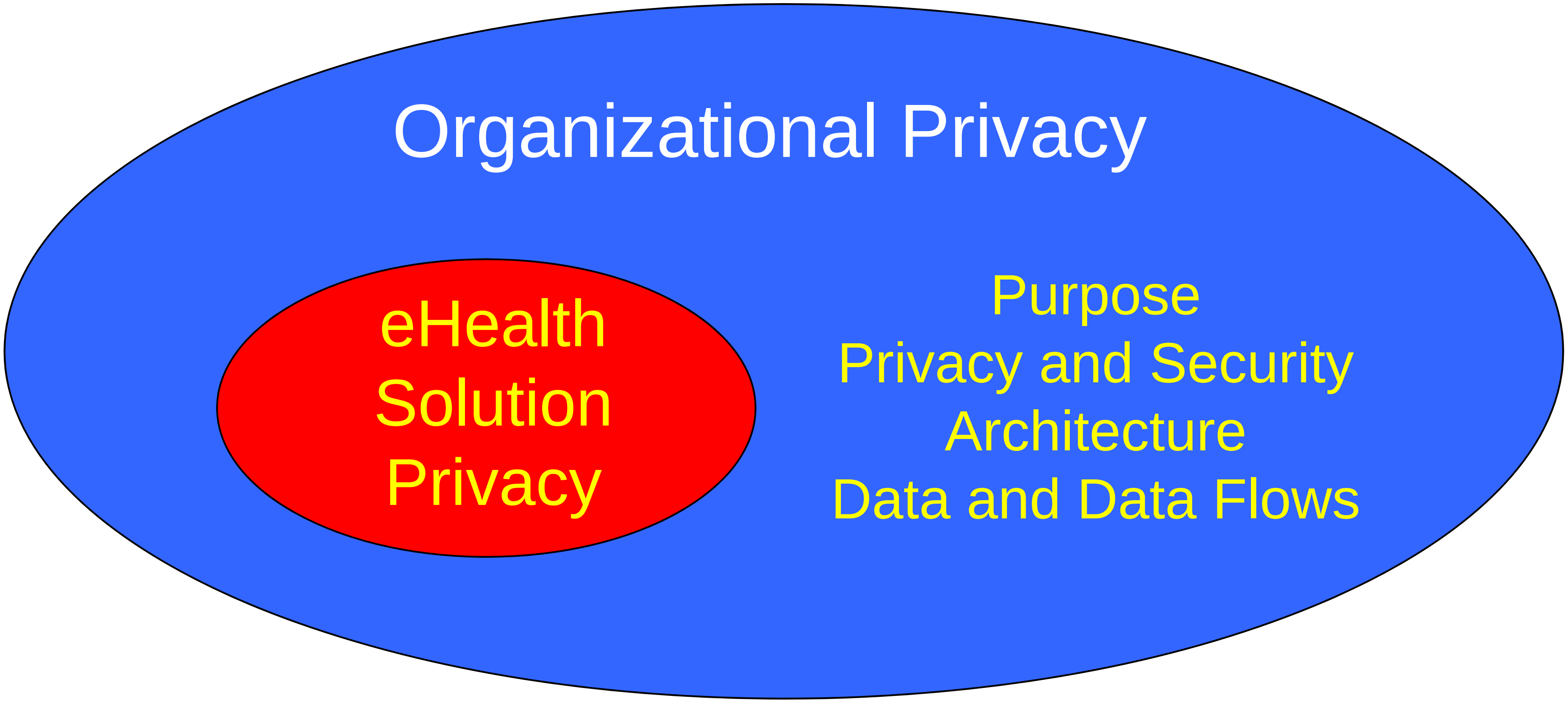
Organizational Privacy

Legislation
Information Governance
Policies and Procedures
Training
Monitoring and Audit

The Privacy Ecosystem



The Privacy Ecosystem



Organizational Privacy

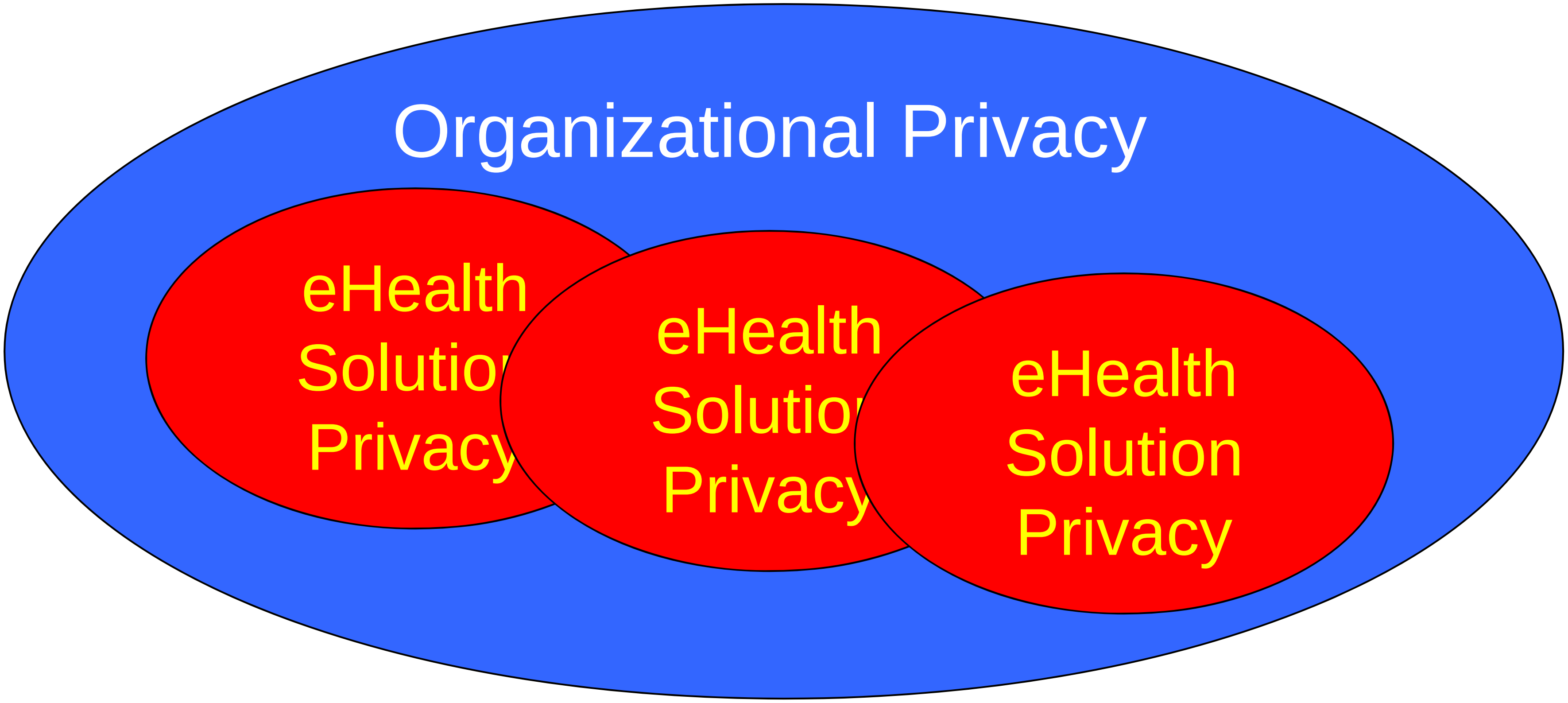
eHealth Solution Privacy

Purpose
Privacy and Security
Architecture
Data and Data Flows

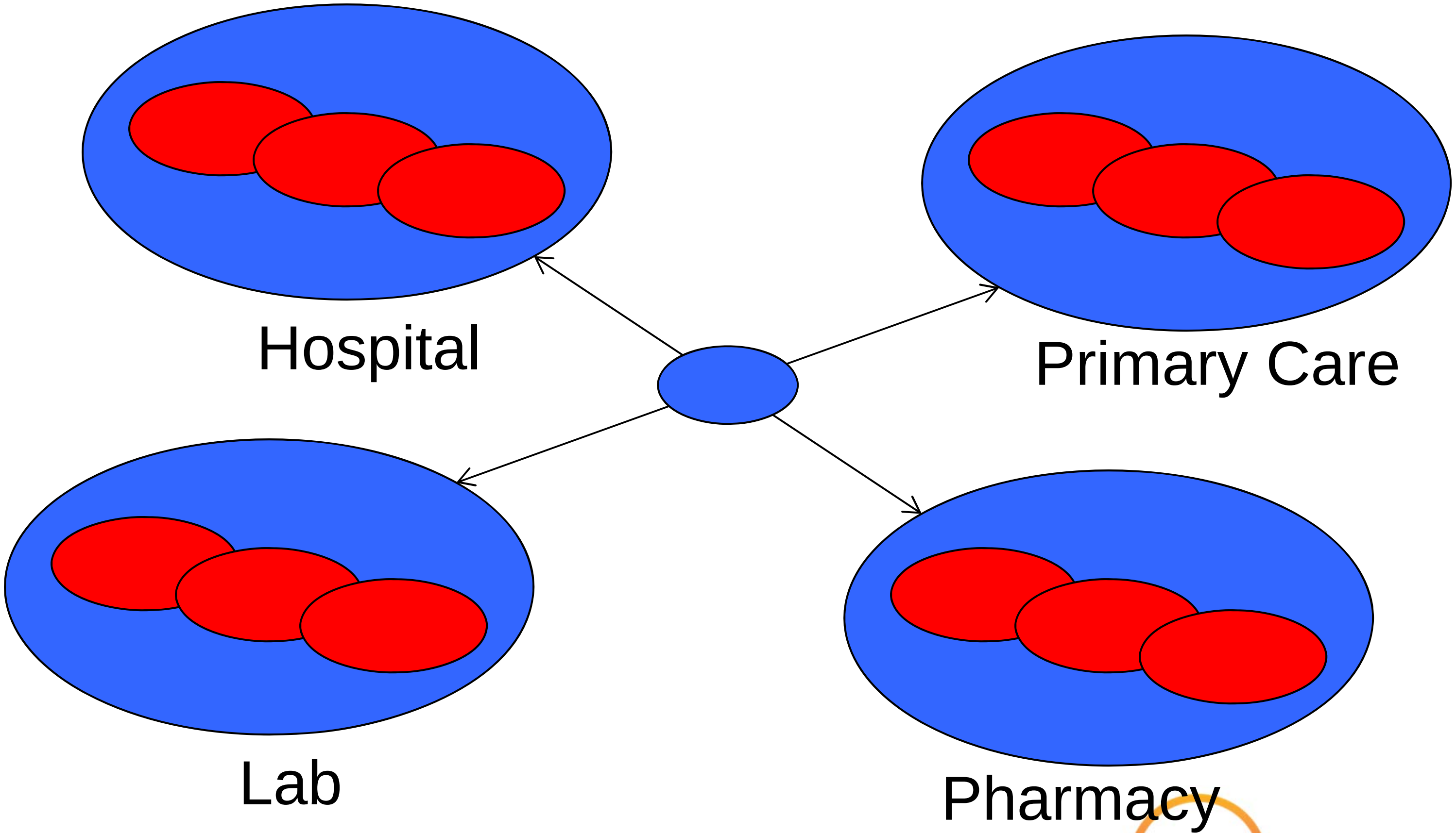
NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

The Privacy Ecosystem



The Privacy Ecosystem



Defining Privacy Requirements

- Legislation
- Control Frameworks
- PIAs & TRAs

Legislation

- Defines patient rights
  - Consent
  - Access to PHI
- Mandates certain administrative practices
  - Privacy Notice/ Statements
  - Breach notification
  - Openness
  - Conditions for collection, use and disclosure

Reasonable and appropriate safeguards

Ontario PHIPA

- 12. (1) A health information custodian shall take steps that are **reasonable** in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

BC - FIPPA

- **30** A public body must protect personal information in its custody or under its control by making **reasonable** security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Alberta HIA

- 60**(1)** A custodian must take **reasonable** steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

  (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information, [More]

- **(2)** The safeguards to be maintained under subsection (1) must include **appropriate** measures

  (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, [More]

Federal PIPEDA

- 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
- Schedule 1, Section 4.7 Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

USA - HIPAA Security Rule

- 164.308(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Reasonable Person Standard

- In the **law** of Negligence, the **reasonable** person standard is the standard of care that a **reasonably** prudent person would observe under a given set of circumstances. An individual who subscribes to such standards can avoid liability for negligence.

So… How do we know what’s reasonable and appropriate?

Determining what’s reasonable

- Apply recognized control frameworks
- Determine required controls based on an assessment of risk
- Create a privacy and security architecture

Example – ISO/IEC 27002

- Physical and Environmental Security
  - Secure area
    - Physical security perimeter
    - Physical entry controls
    - Securing offices, rooms and facilities
    - Protecting against external and environmental threats
    - Working in secure areas
    - Public access, delivery, and loading areas

Privacy Control Frameworks

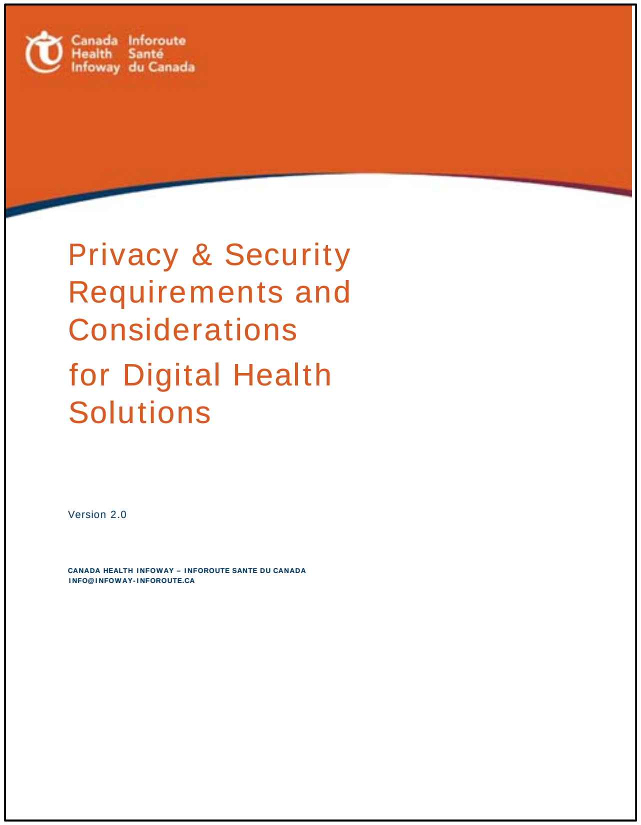
- ISO/IEC 29100:2011 – Privacy Framework
- CSA Model Code for the Protection of Personal Information
- AICPA/CICA Generally Accepted Privacy Principles
- OECD Guidelines on the Protection of Privacy and Transborder flows of Personal data

Security Control Frameworks

- ISO/IEC 27002:2013 – Code of Practice for Information Security Management
- ISO 27799 – Information security management in health using ISO/IEC 27002
- ISO/IEC 27018:2014 – Code of Practice for Protection of PII in public clouds''
- NIST Introductory Resource Guide for Implementing the HIPAA Security Rule

EHR Privacy & Security Requirements

- Canada Health Infoway
- Comprehensive guide to privacy and security in EHRs
- Based on CSA Privacy Code and ISO 27002 and 27799



Canada Health Infoway
Inforoute Santé du Canada

Privacy & Security Requirements and Considerations
for Digital Health Solutions

Version 2.0

CANADA HEALTH INFOWAY – INFOROUTE SANTE DU CANADA
INFO@INFOWAY-INFOROUTE.CA

Sample EHR requirements

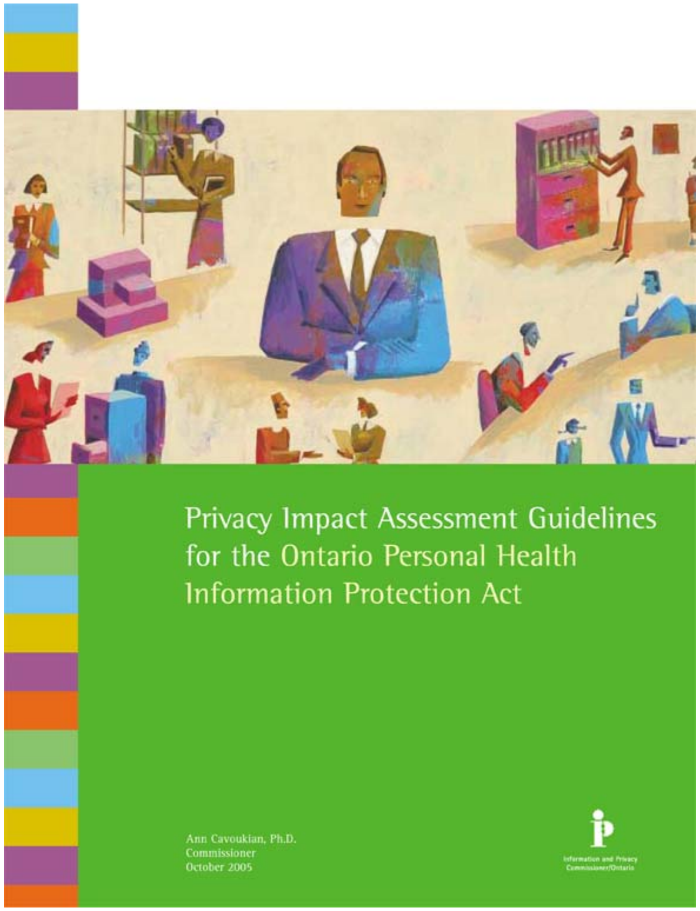
- Privacy Requirements
  - Recording consent
  - Logging access, modification and disclosure
  - Retaining records
  - Flagging records at high risk

- Security Requirements
  - Access control
  - Authenticating users
  - Validating input data
  - Encryption
  - Portable media
  - Audit logging
  - Password management

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

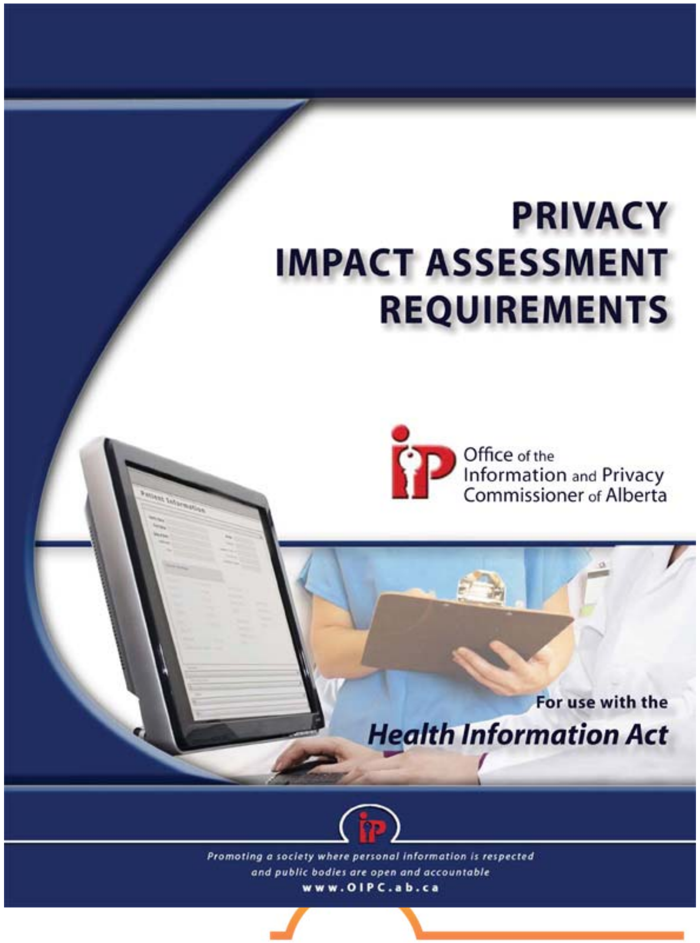
The PIA and TRA as Tools for PbD



Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Information and Privacy Commissioner/Ontario



PRIVACY
IMPACT ASSESSMENT
REQUIREMENTS

Office of the Information and Privacy Commissioner of Alberta

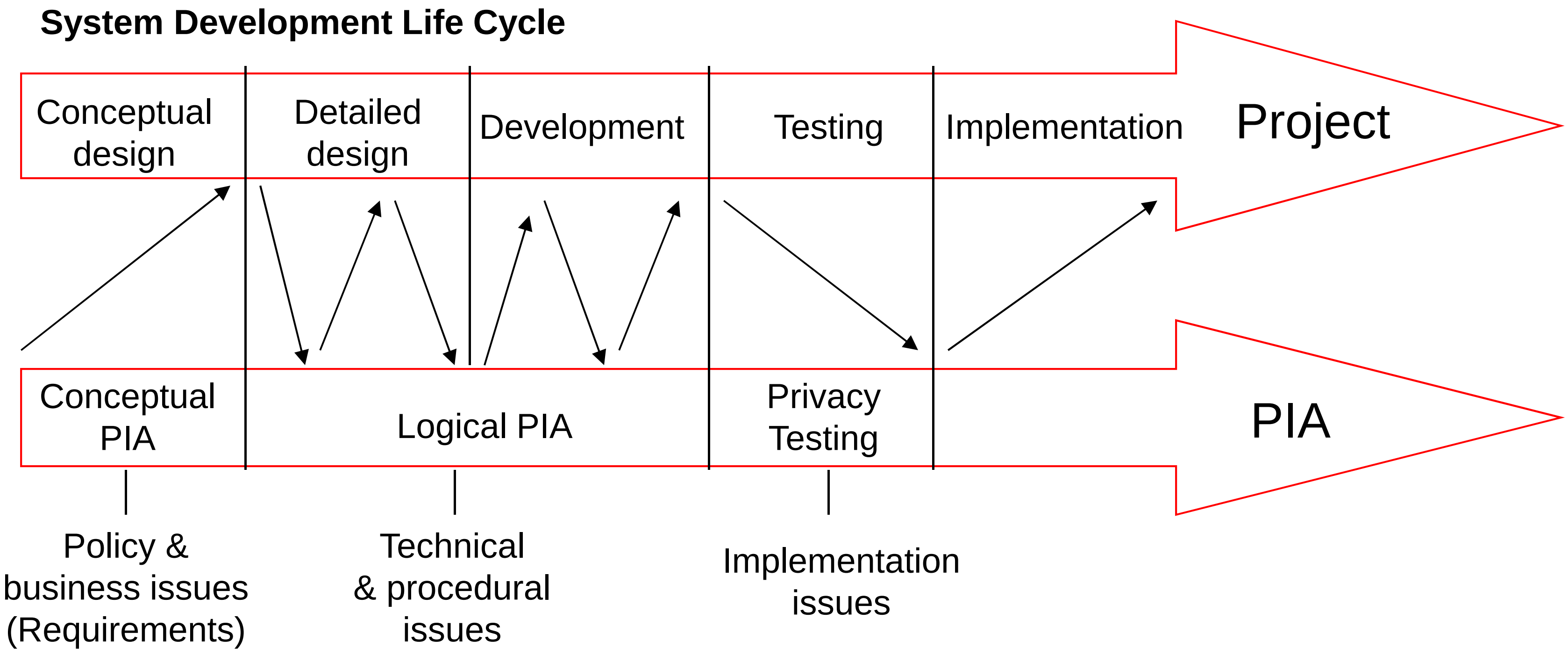
For use with the
Health Information Act

Promoting a society where personal information is respected and public bodies are open and accountable
www.OIPC.ab.ca

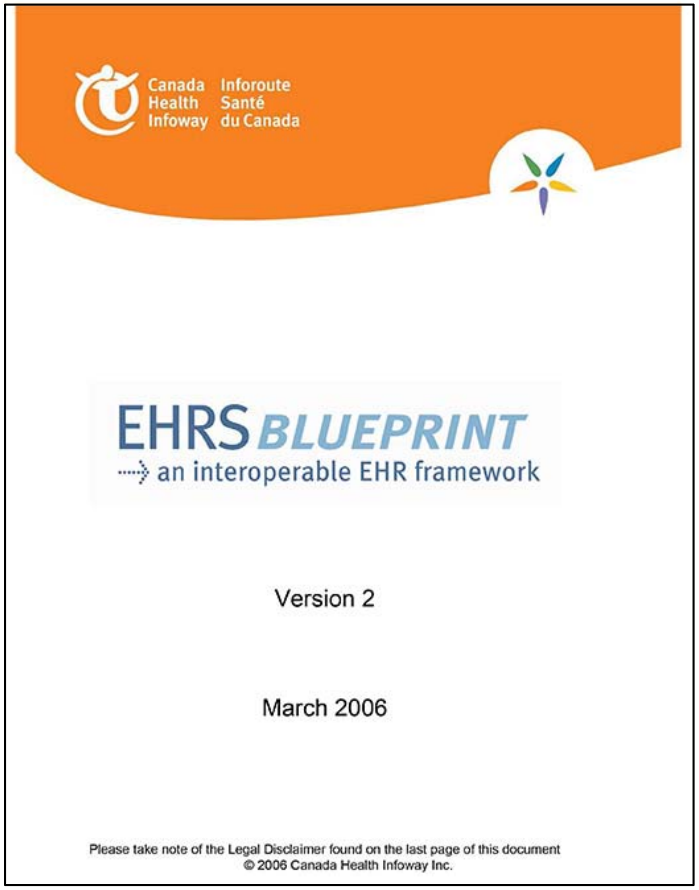
NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

The PIA and TRA as Project Management Tools



Privacy & Security Architecture



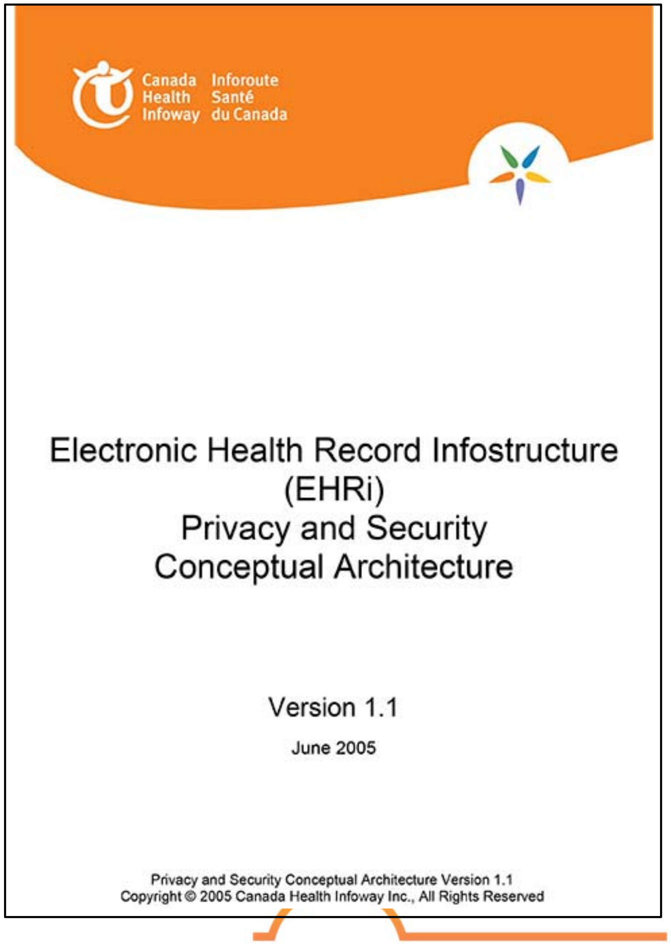
Canada Health Infoway
Inforoute Santé du Canada

EHRS BLUEPRINT
an interoperable EHR framework

Version 2

March 2006

Please take note of the Legal Disclaimer found on the last page of this document
© 2006 Canada Health Infoway Inc.



Canada Health Infoway
Inforoute Santé du Canada

Electronic Health Record Infostructure
(EHRi)
Privacy and Security
Conceptual Architecture

Version 1.1

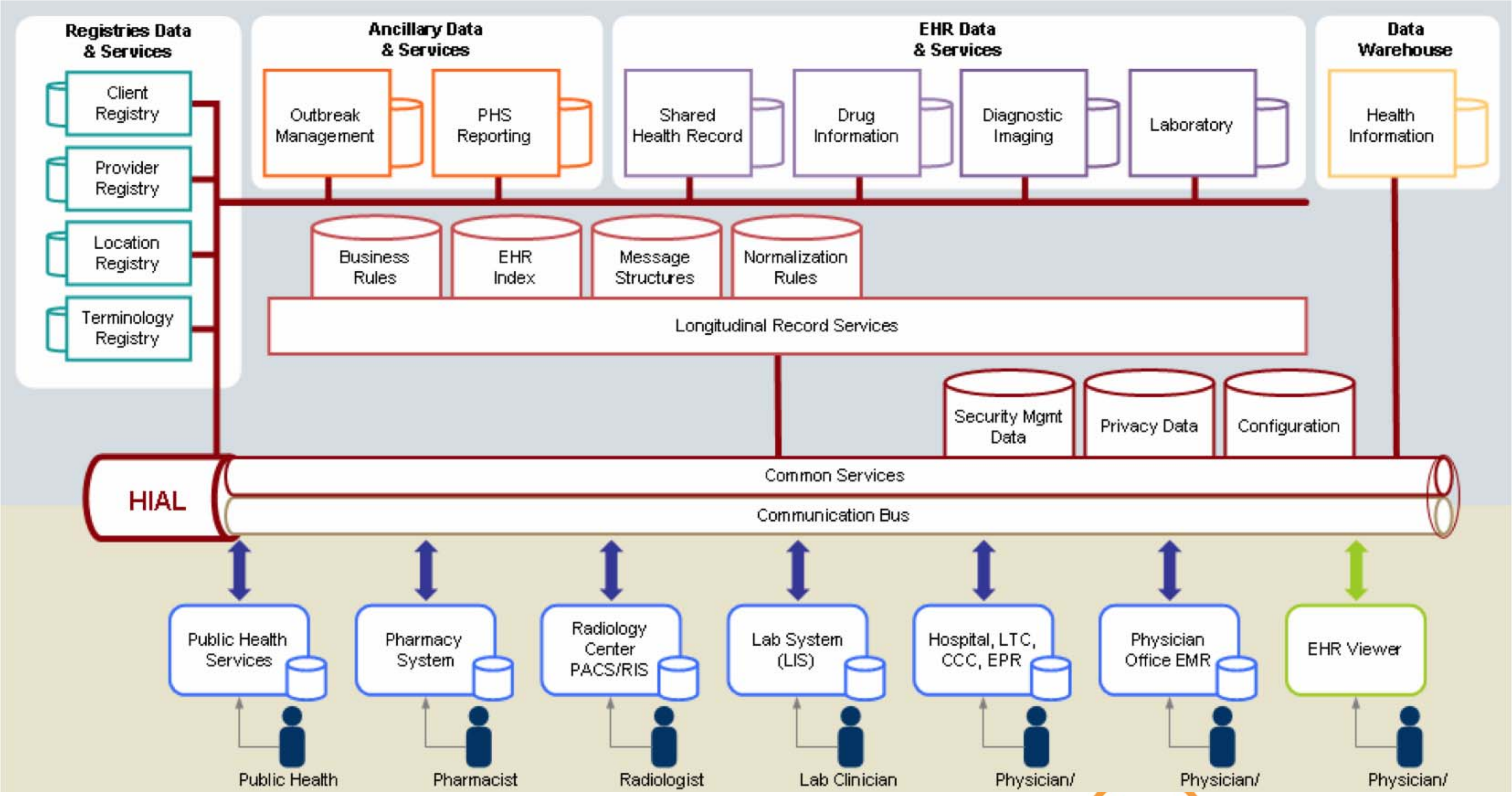
June 2005

Privacy and Security Conceptual Architecture Version 1.1
Copyright © 2005 Canada Health Infoway Inc., All Rights Reserved

NiHi CANADA National Institutes of Health Informatics

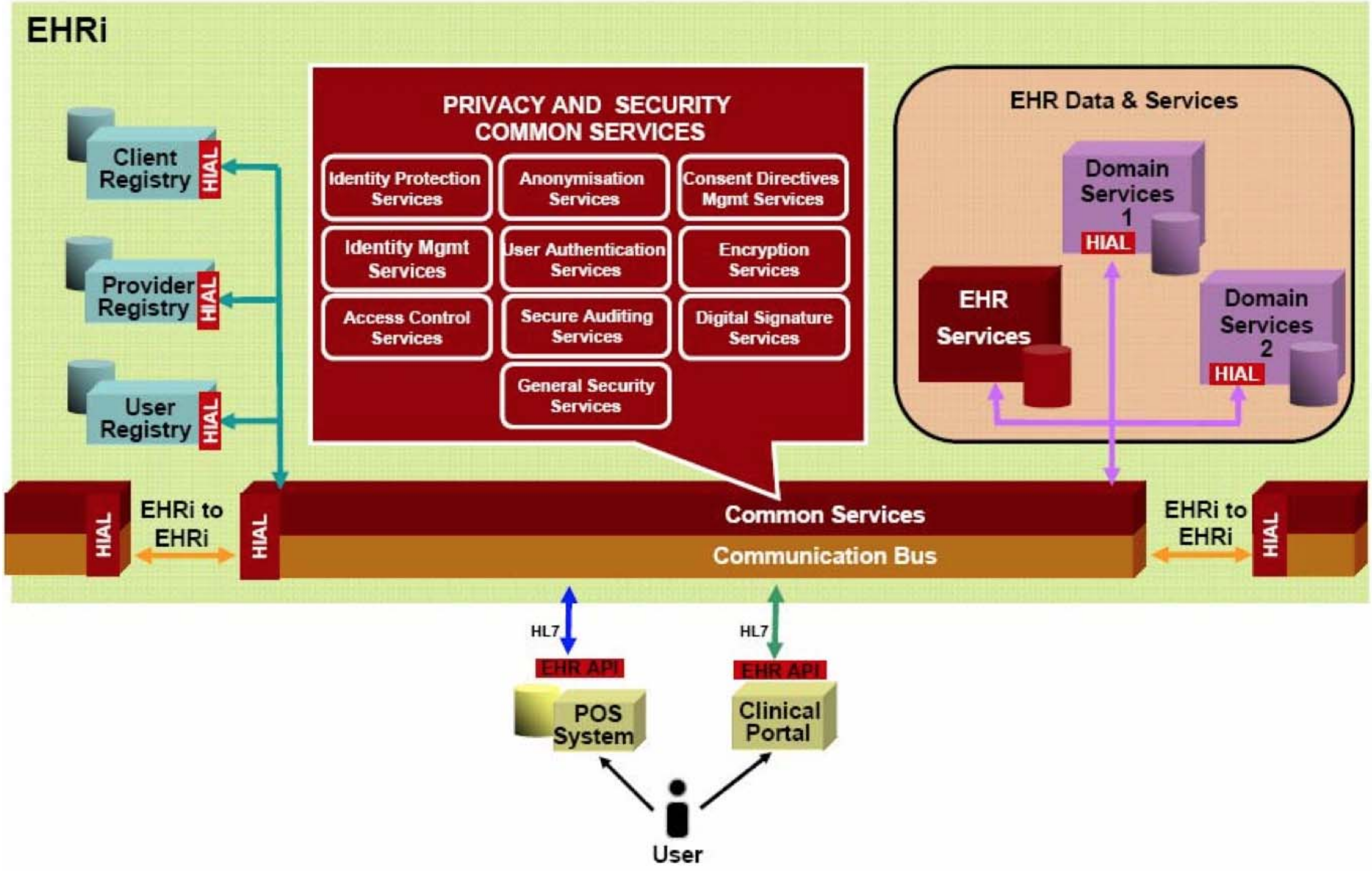
Privacy Horizon

Privacy & Security Architecture EHRS Conceptual Overview

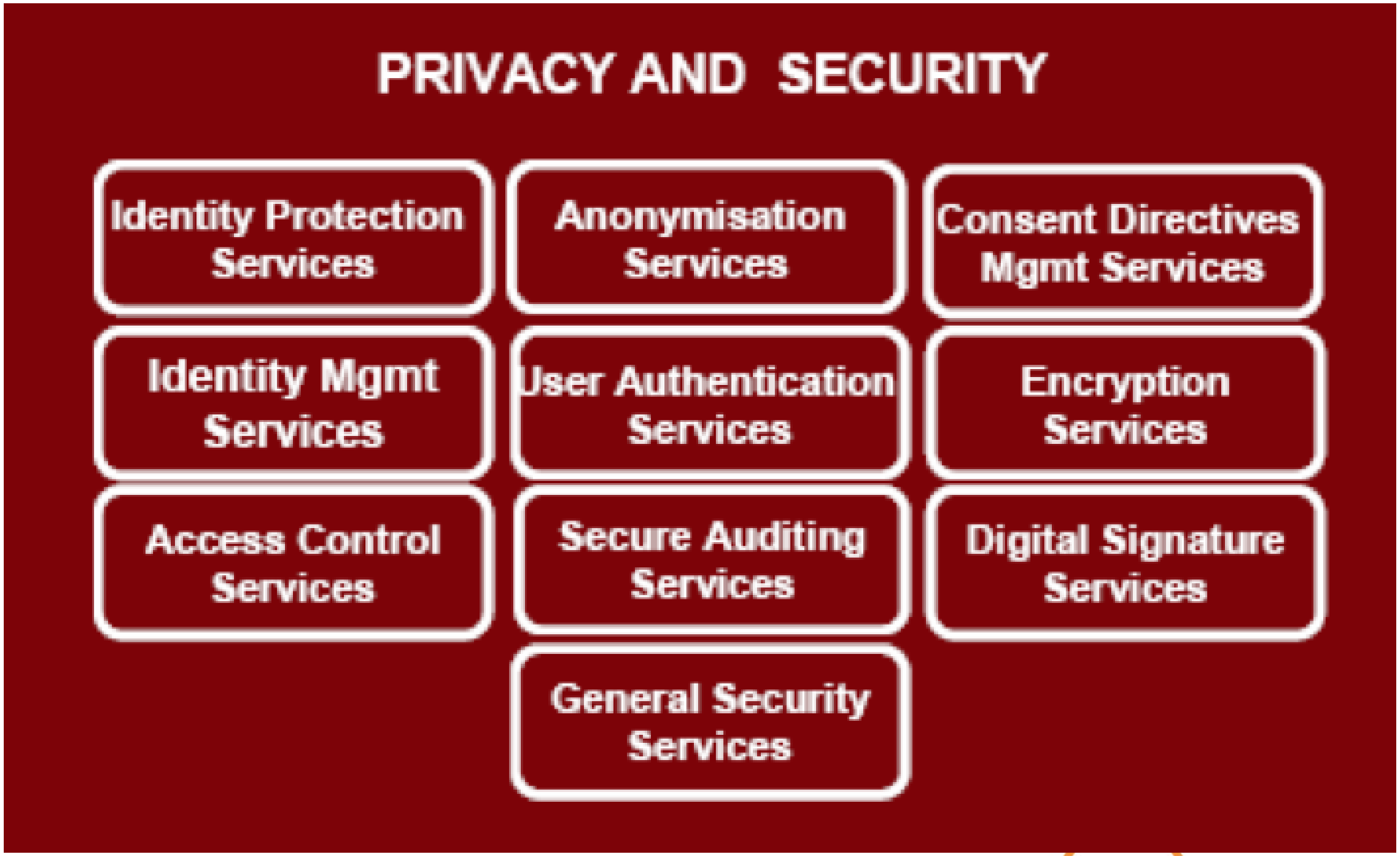


NiHi CANADA National Institutes of Health Informatics

Privacy Horizon


EHRi
Client Registry
HIAL
Provider Registry
HIAL
User Registry
HIAL
PRIVACY AND SECURITY COMMON SERVICES
Identity Protection Services
Anonymisation Services
Consent Directives Mgmt Services
Identity Mgmt Services
User Authentication Services
Encryption Services
Access Control Services
Secure Auditing Services
Digital Signature Services
General Security Services
EHR Data & Services
Domain Services 1
HIAL
EHR Services
Domain Services 2
HIAL
HIAL
EHRi to EHRi
HIAL
Common Services
Communication Bus
EHRi to EHRi
HIAL
HL7
HL7
EHR API
EHR API
POS System
Clinical Portal
User

Privacy & Security Architecture



PRIVACY AND SECURITY

Identity Protection Services

Anonymisation Services

Consent Directives Mgmt Services

Identity Mgmt Services

User Authentication Services

Encryption Services

Access Control Services

Secure Auditing Services

Digital Signature Services

General Security Services

NiHi CANADA National Institutes of Health Informatics

Privacy Horizon

Summary

- Legislation (What we must do!)
- Control Requirements (what we should do!)
- Privacy and Security Architecture (how do we do it?)
- P&S Risk Assessment (What should we do first?)

SOUND REASONABLE?

QUESTIONS?