

# Implementing ISO 17799 in Alberta's Health Sector



---

---

---

---

---

---

---

---

---

---

## Overview

- Environment
- Our experience - History
- Current approach
- Success factors
- Future direction
- Q&A



---

---

---

---

---

---

---

---

---

---

## Environment



---

---

---

---

---

---

---

---

---

---

## Legislation

- Health Information Act (2001)
- Duty to protect health information:
  - Must assure confidentiality, integrity and availability
  - Must have policies
  - Must name a security authority
  - Employee/contractor awareness
  - Periodic review of controls
  - Special mention of electronic records
  - Special mention of out-of-province safeguards

4

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

## Organization of Health Sector

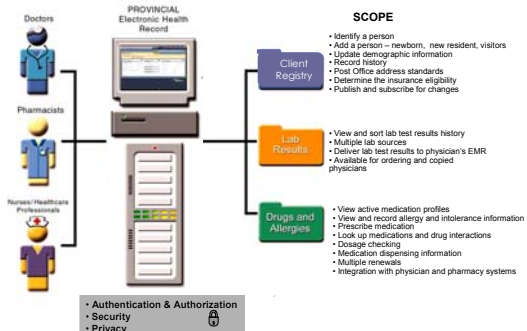
- Alberta Health and Wellness
  - Alberta Wellnet
- 9 Regional Health Authorities
- Cancer Board, Mental Health Board
  - Provincial mandates
- Highly decentralized
- All considered ‘custodians’ under Health Information Act

5

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

## Provincial Electronic Health Record



6

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

## Other electronic health records



- Calgary Health Region
  - Eclypsis
- Capital Health (Edmonton)
  - netCare
- Cancer Board
  - Optx
- Non-Metro Health Regions
  - Meditech

7

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

## History



8

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

## Our Experience - History



- 2000- AHW IT Operations leads security
  - 2 Privacy & Security Offices – AHW and Wellnet
- Health Authorities encouraged to adopt BS 7799
- May ~~October~~ 2000 telephone assessments
  - HA's expected to write policies, create security 'role'
- 2001- AHW develops 'security policy template'
  - Based on BS 7799
  - Encouraging approach (no carrot, no stick)
- Spring/Summer 2002 – Minimum Connectivity Requirement
  - Subset of 7799, focused on access/network/communication controls
  - Minimum controls to connect to AHW applications without Fobs

9

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

## Our Experience - History (continued)



- September 2002 – AHW IM leads security strategy
  - IT operations implements security measures
  - Wellnet Privacy & Security office brought under AHW
- December 2002 – AHW conducts on site gap analysis of MCR
  - Objective: determine gaps between written policies and practice
  - Results show that no HA is in compliance
  - Provincial EHR rolling out
- February 2003 – Security grants announced
  - \$4 million, distributed by population formula
  - HAs given until December 31, 2003 to comply with MCR
  - Verification currently underway
  - Carrot is grant, stick is provincial EHR access

10

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---

## Current Approach



11

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---

## Current Approach



- Phased approach to implementing ISO controls
- 50% of remaining controls over next two years
  - 2004-05 and 2005-06
  - Order based on risk
- Cycle of approvals same each year
  - Announce annual funding
  - AHW approves security plans, releases 85% funding
  - RHAs/Boards implement plans, report monthly
  - RHAs/Boards submit final report
  - AHW verifies, releases remaining 15%

12

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---

## Phased implementation of ISO controls



- Minimum Connectivity Requirement
  - Access control
  - Communications and operations management
  - Some organization, personnel, physical and compliance controls
- Remaining controls are fairly evenly split on subject area
- 2004 5 Controls emphasize:
  - Policy and organization controls
  - More communications and operations management
- 2005 6 Controls emphasize:
  - Physical controls
  - Business continuity

13

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

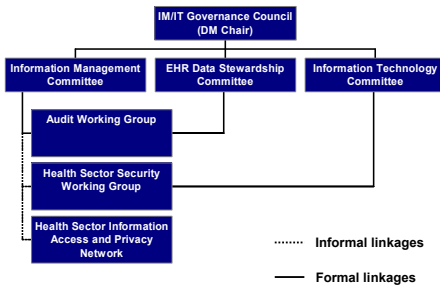
---

---

---

---

## Governance



14

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

## Other initiatives



- Security requirements for physician offices
  - Physician Office System Program
  - Vendor Conformance and Usability Requirements (VCUR) (includes security requirements)
  - Funding tied to VCUR compliance
- Security requirements for pharmacies
  - Under discussion
- Authentication and Authorization
  - Alberta Secure Access Service
- Self assessment tool
  - Privacy and security compliance
  - Based on MCR – will add remaining ISO controls over next 2 years

15

ISO 17799 User Group Canada / Infosec Canada – June 1, 2004

Alberta Health and Wellness

---

---

---

---

---

---

---

---

# Success Factors



---

---

---

---

---

---

---

---

## Success factors - general



- Establish executive level privacy & security steering committee
- Create technical expertise in IT security in sector
- Adopt a common approach to extending trust
- Ensure privacy and security offices are in contact with each other
- Dedicate funding

---

---

---

---

---

---

---

---

## Our conditions for success



- Health Information Act
  - Provides authority
- Office of the Information and Privacy Commissioner
  - Informed and supportive
- Electronic Health Records
  - Substantial investment
  - Concerns over privacy and security would put initiative at risk
- AHW willingness to provide dedicated resources

---

---

---

---


---

---

---

---

Future Direction



19 ISO 17799 User Group Canada / Infosec Canada – June 1, 2004 Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---

Future Direction

- Establish common privacy and security strategy
  - Information Security Management System (ISMS)
- Mandatory self-assessment
  - 2005-06
- Monitoring provincial EHR
  - Checking system logs against patient charts

20 ISO 17799 User Group Canada / Infosec Canada – June 1, 2004 Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---

Q&A

Brian Hamilton  
Manager, Privacy & Security  
Alberta Health & Wellness  
[brian.hamilton@gov.ab.ca](mailto:brian.hamilton@gov.ab.ca)  
(780) 422-5111

21 ISO 17799 User Group Canada / Infosec Canada – June 1, 2004 Alberta Health and Wellness

---

---

---

---

---

---

---

---

---

---