

Implementing ISO 17799 in Health

Brendan Seaton
Chief Privacy and Security Officer
Smart Systems for Health Agency
June 14, 2005

PRIVACY
OFFICER



SLANE

17799 in Health

- The Smart Systems for Health Agency
- The Advantages of using ISO 17799 in the health care environment
- The demands of the Ontario Personal Health Information Protection Act and other privacy legislation
- The initiative by the Ontario Health Information Standards Council (OHISC) to adopt key provisions of ISO 17799
- The development of ISO 27799 – an international standard that adapts ISO 17799 to the health care environment
- A case study – implementing ISO 17799 at the Ontario Smart Systems for Health Agency

SSHA: Transforming Healthcare through IT

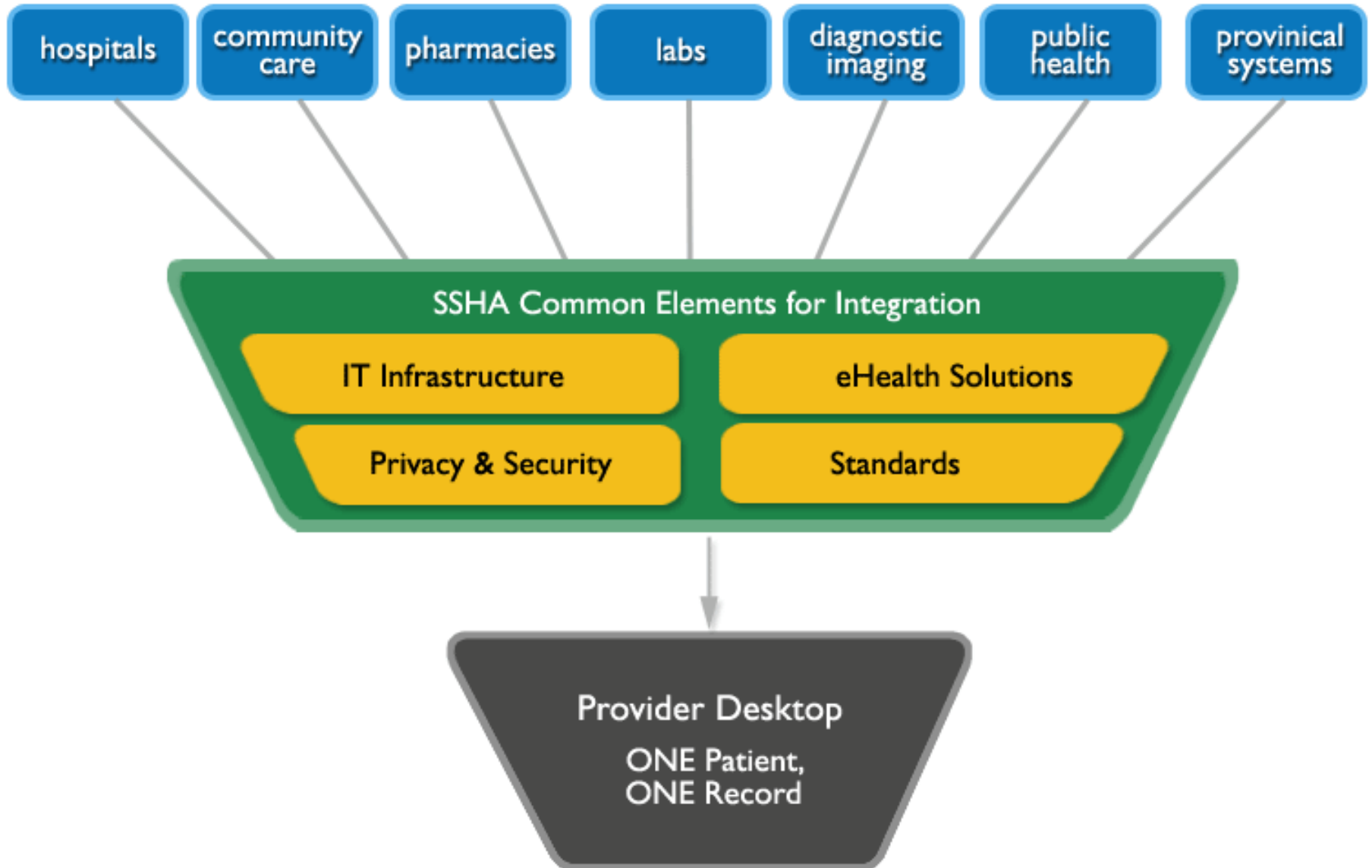
- Providing healthcare providers with timely, secure electronic access to patient information
- Creating a secure patient information sharing network between 150,000 providers at 24,000 sites
- The results:
 - Improved patient care
 - More effective providers
 - Integration
 - Better use of financial resources

SLANE

What SSHA is not!



e-Health Success



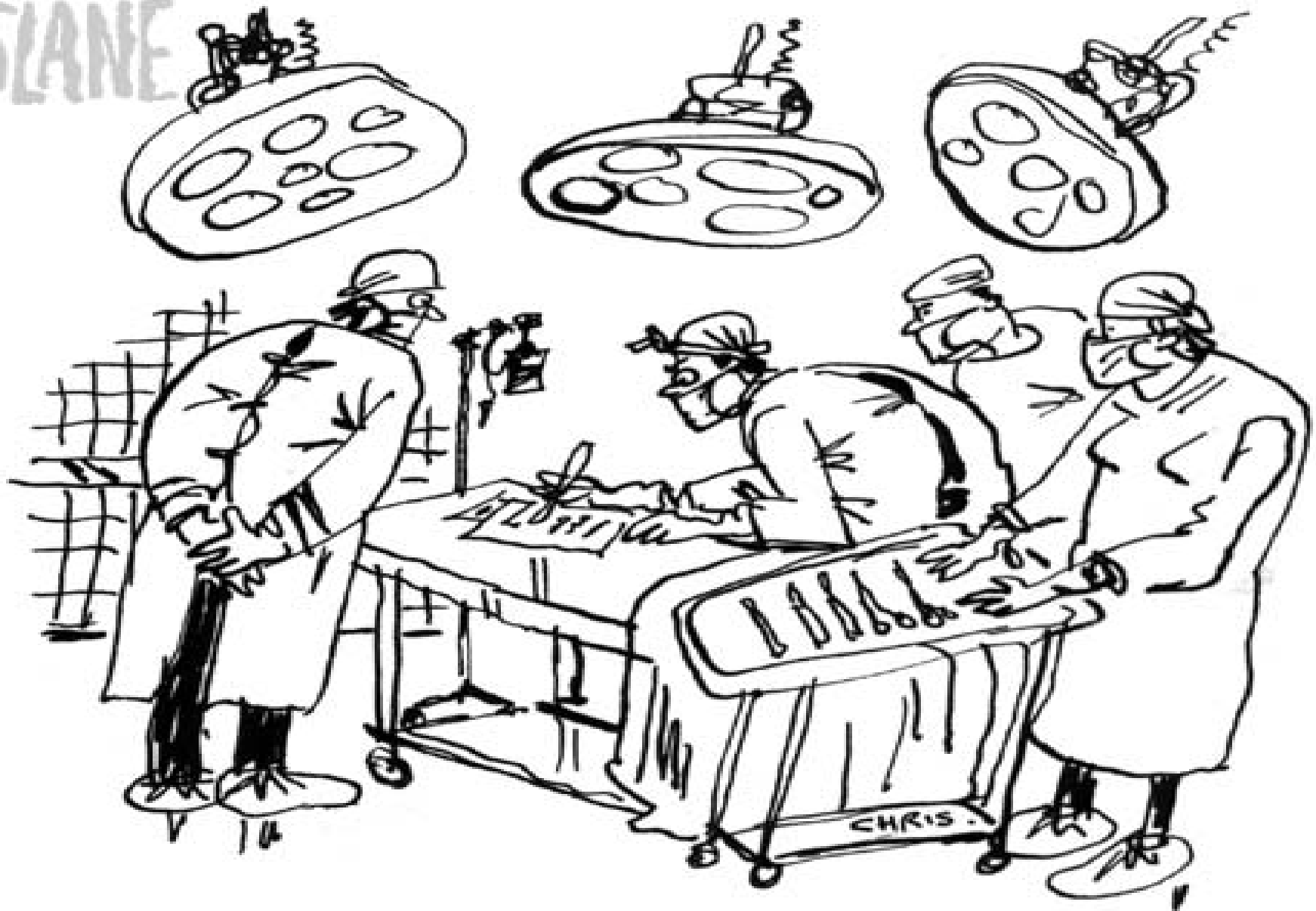


Advantages of using 17799 in health

- Its the most readable and reachable security standard out there
- Widely deployed in health care
- Technology independent
- Ability to “certify” compliance
- No one ever got fired for implementing an ISO standard

Demands of Privacy Legislation

- Complex matrix of privacy legislation in Ontario and across Canada
 - PHIPA
 - FIPPA
 - PIPEDA
- Focus on rights of individuals and obligations of information custodians
- Significant responsibility defined for security but little guidance



I AM NOW CUTTING ALL MY RUDE
REMARKS ABOUT THE PATIENT FROM HER FILE.

Adoption of 17799 for Ontario Health

- Proposal currently before the Ontario Health Information Standards Council (OHISC)
- Adopts 3 key sections of ISO 17799: 2004
 - Risk Assessment
 - Security Management
 - Security Policy
- SSHA to develop implementation toolkit including:
 - Risk assessment methodology
 - Policy templates
 - Training and education programs

ISO 27799

- ISO 27799 is an international standard being developed to promote ISO 17799 in health
- Being developed by ISO/TC215/WG4 – Health Information Security
- Provides useful guidance on the application of 17799 control statements in the health care environment
- Identifies key provisions as “normative” or mandatory in health care
- At committee draft stage – International standard is 12 to 24 months away.

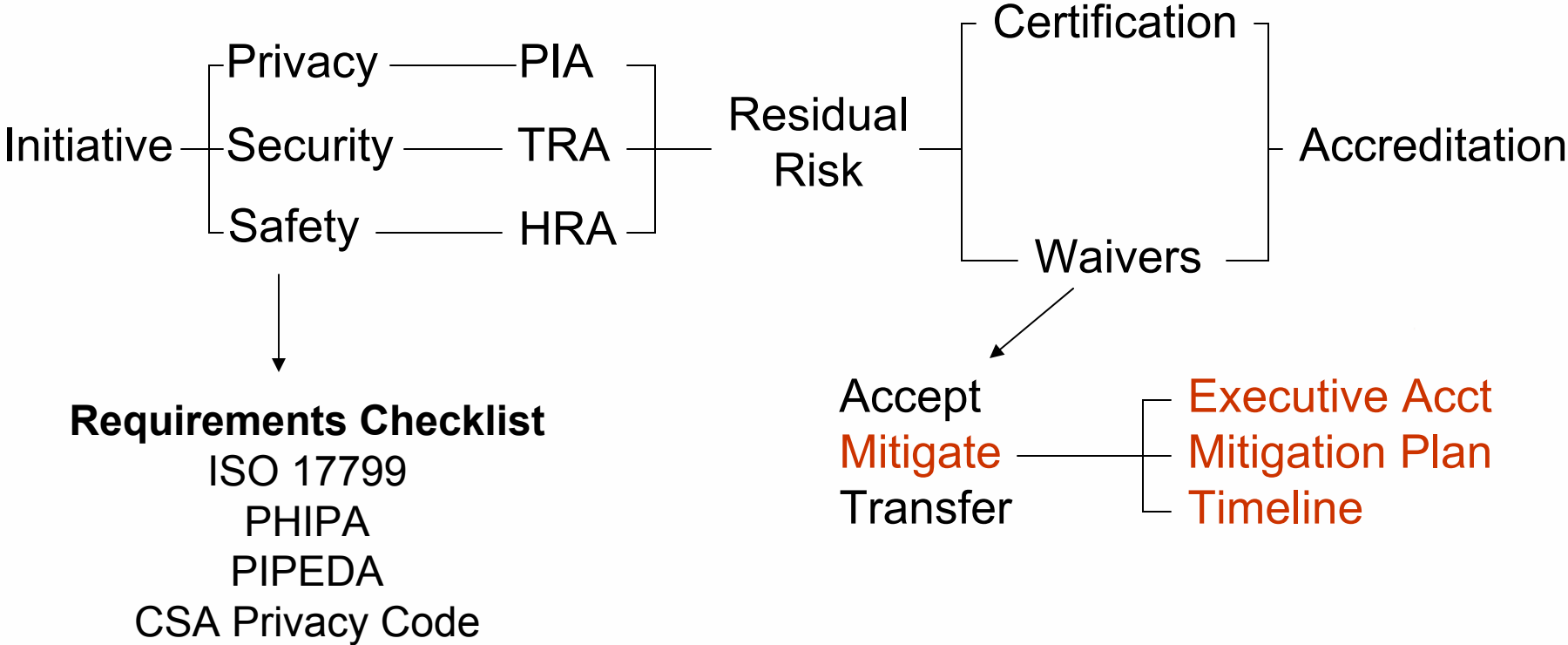
Implementing ISO 17799 at SSHA

- Information security program is based on ISO 17799
- SSHA follows 17799's guidance for security policy and management
- Threat and risk assessment methodology based on CSE and NIST
- 17799 control statement checklist forms part of the certification and accreditation program

Certification and Accreditation

- *Balancing operational demands and risks*
- *Based on CSE MG4 C&A Methodology*
- *Establishing Certification and Accreditation Authorities*
- *Managing risks – accept, mitigate and transfer*
- *Establishing executive accountability for security, privacy and safety risk management*

Risk Management Framework



Your Questions

brendan.seaton@ssha.on.ca

(416) 586-4209

www.ssha.on.ca