

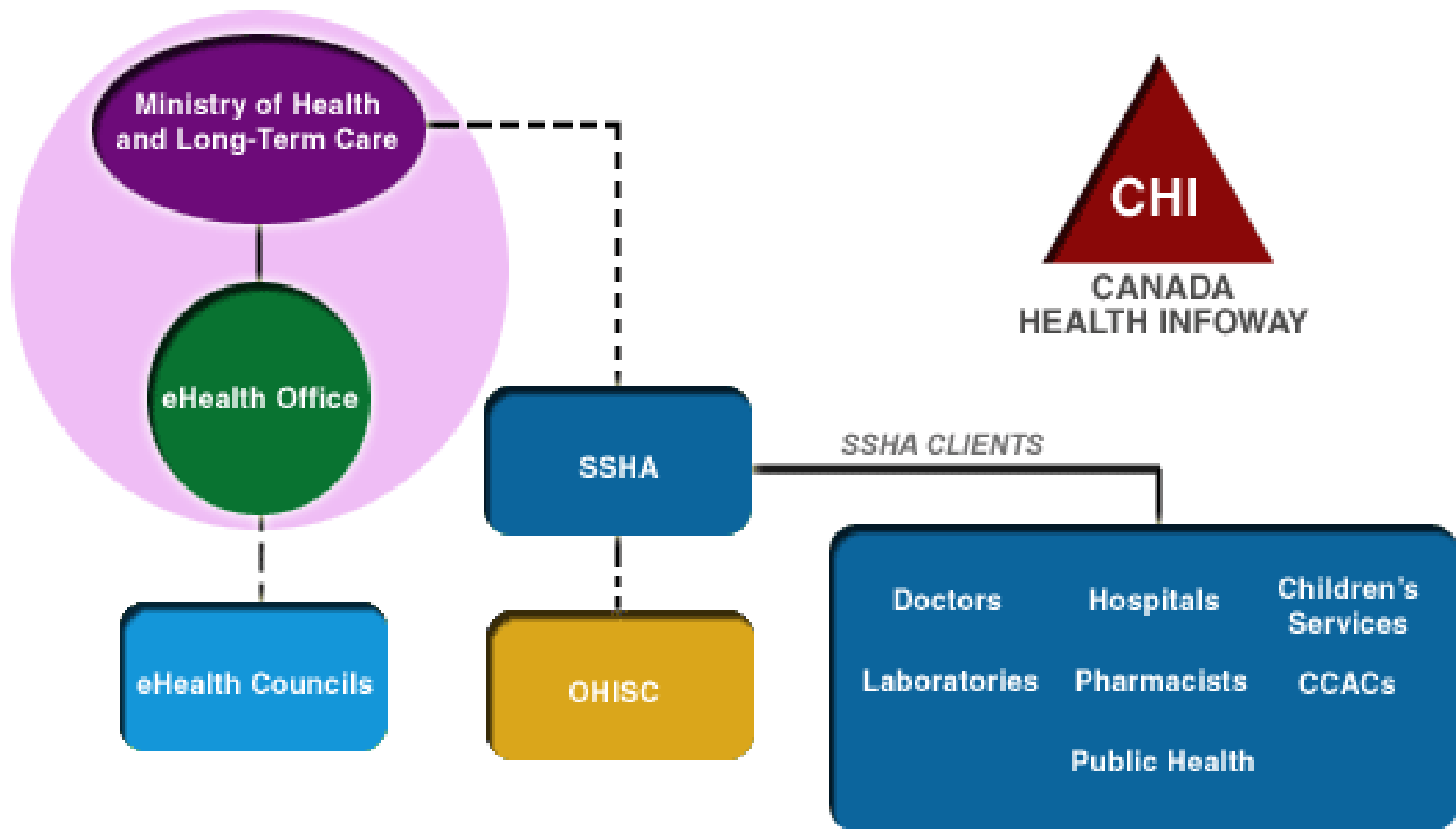
Managing Risk in Health Information Systems

*Michael Connolly, Brendan Seaton
Smart Systems for Health Agency
May 25, 2005*

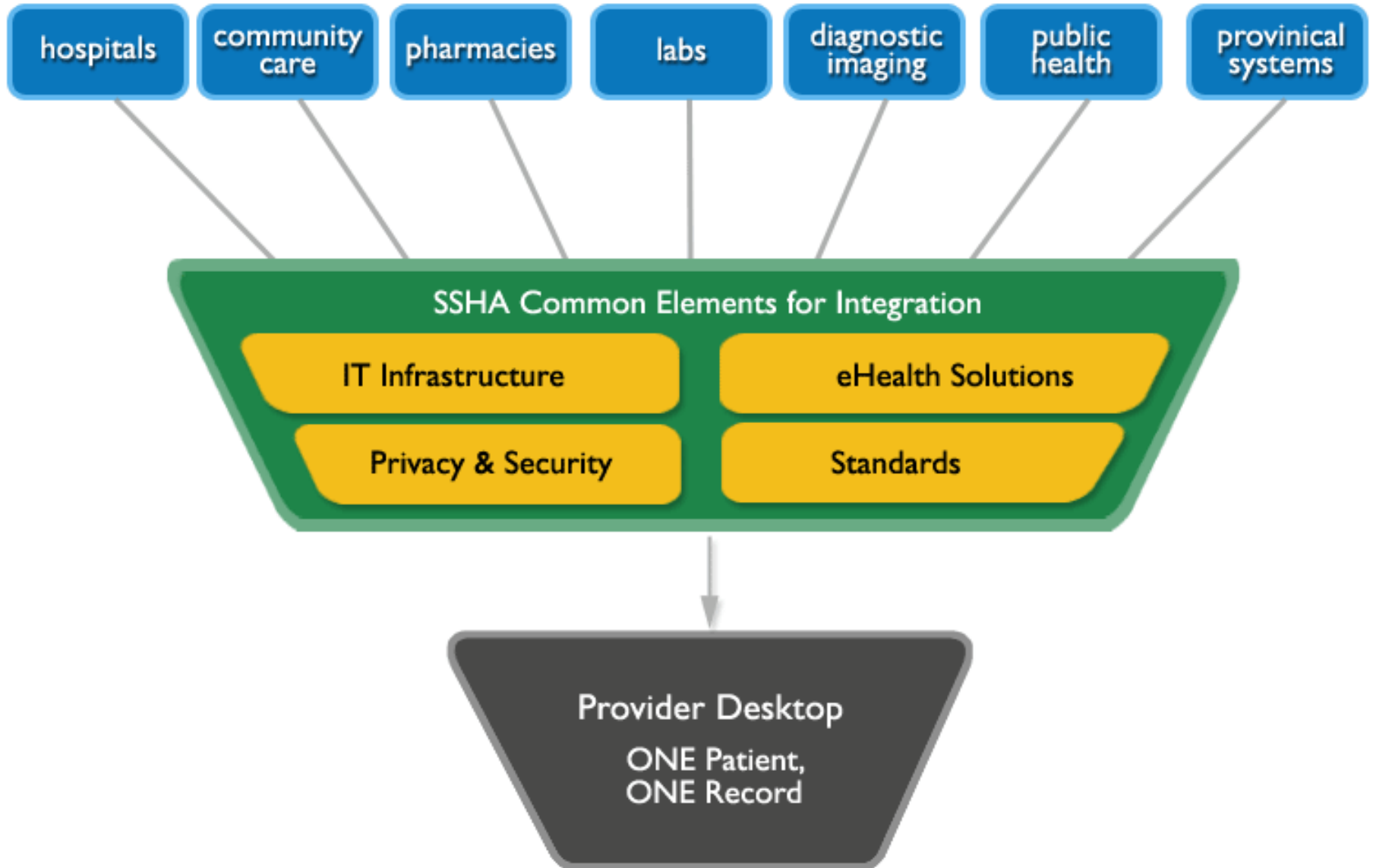
Managing Risk

- A Vision for eHealth
- Managing Risk at SSHA
- The Road Ahead

eHealth in Ontario



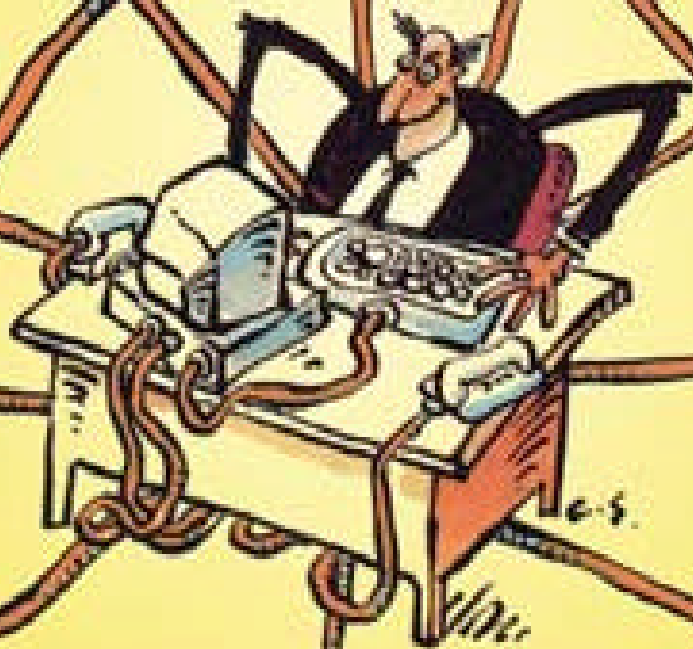
e-Health Success



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

What SSHA is not!



SSHA Background

- Mandate
 - Establish and operate the common IT infrastructure for the healthcare system
 - Provide e-Health business solutions
- How we carry it out
 - MOHLTC approved priority initiatives
 - Trusted third party for healthcare providers to securely share patient information

IT Infrastructure

- Core technologies needed by all applications
 - A place for them to live ... data centres
 - A way to move information around ... network
 - Controls on who can use them ... security
 - Someone to look after them ... support

SSHA Products and Services

- Secure Hosting
- Network Services
- Portal Services
- Secure Email
- Registration Services
- Contact Centre
- Electronic Health Record
- Standards Management
- Privacy and Security

Who is eligible?

- Hospitals
- Pharmacists
- Laboratories
- Physicians
- Nurses
- Nurse Practitioners
- Public Health Units
- Community Care Access Centres
- Ministry of Health and Long-Term Care programs
- Long Term Care Facilities
- Children's Treatment Centres
- Independent Health Facilities
- Community Support Agencies
- Substance Abuse / Addiction Agencies
- Clinics
- Homes for Special Care
- Aboriginal Health Centres

Managing Risk in SSHA Products and Services

- SSHA addresses risk in the areas of:
 - Privacy
 - Security
 - Safety
- All products and services subject to certification and accreditation

Managing Risk – Tools and Techniques

- Privacy, Security, and Safety design principles
- Privacy Impact Assessment
- Threat and Risk Assessment
- Hazard Risk Assessment
- Certification and Accreditation

Privacy/ Security/ Safety Design Principles

- More economical to build privacy, security and safety into the design process (system or program) than after the fact
- Good business practices
- Good information management practices

Patient Interests



Confidentiality

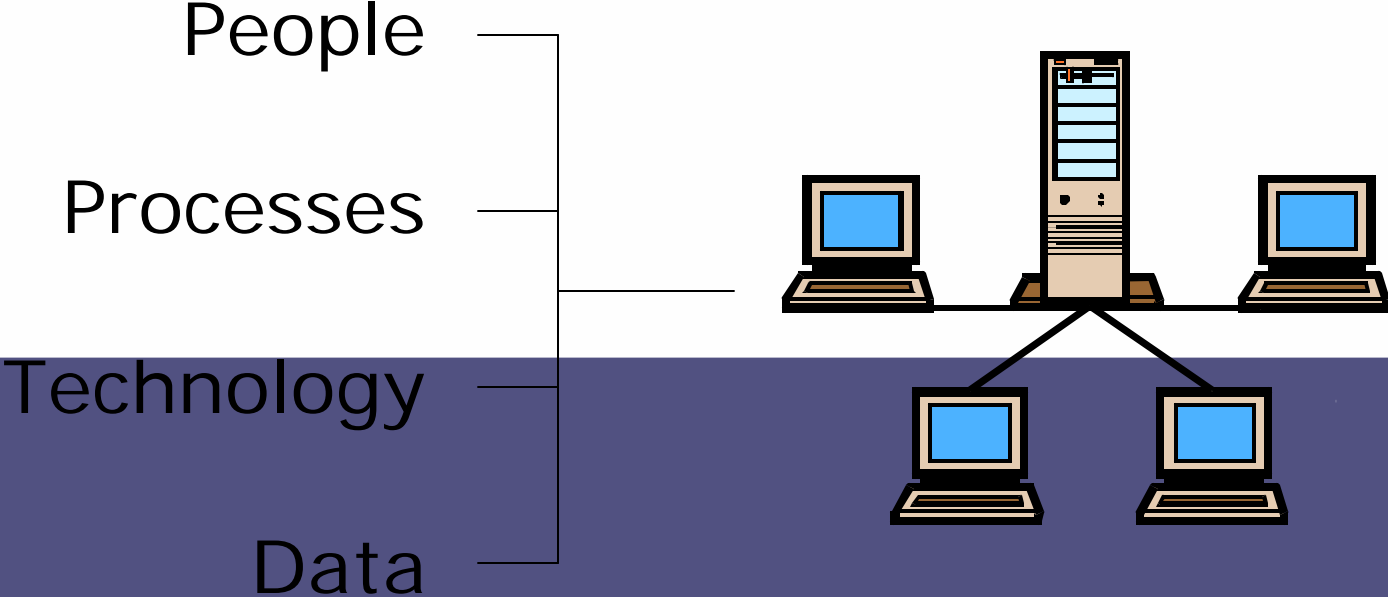
Availability

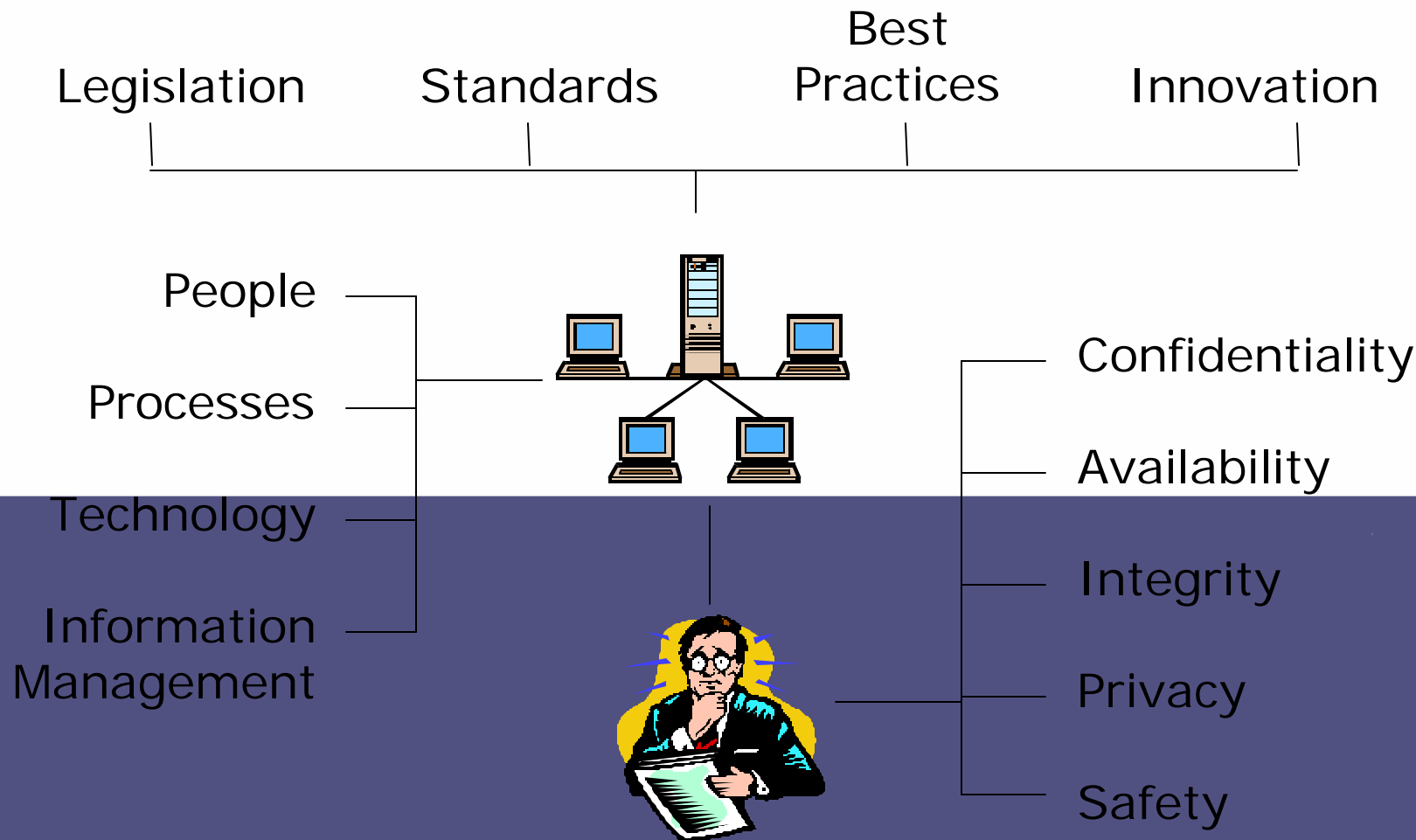
Integrity

Privacy

Safety

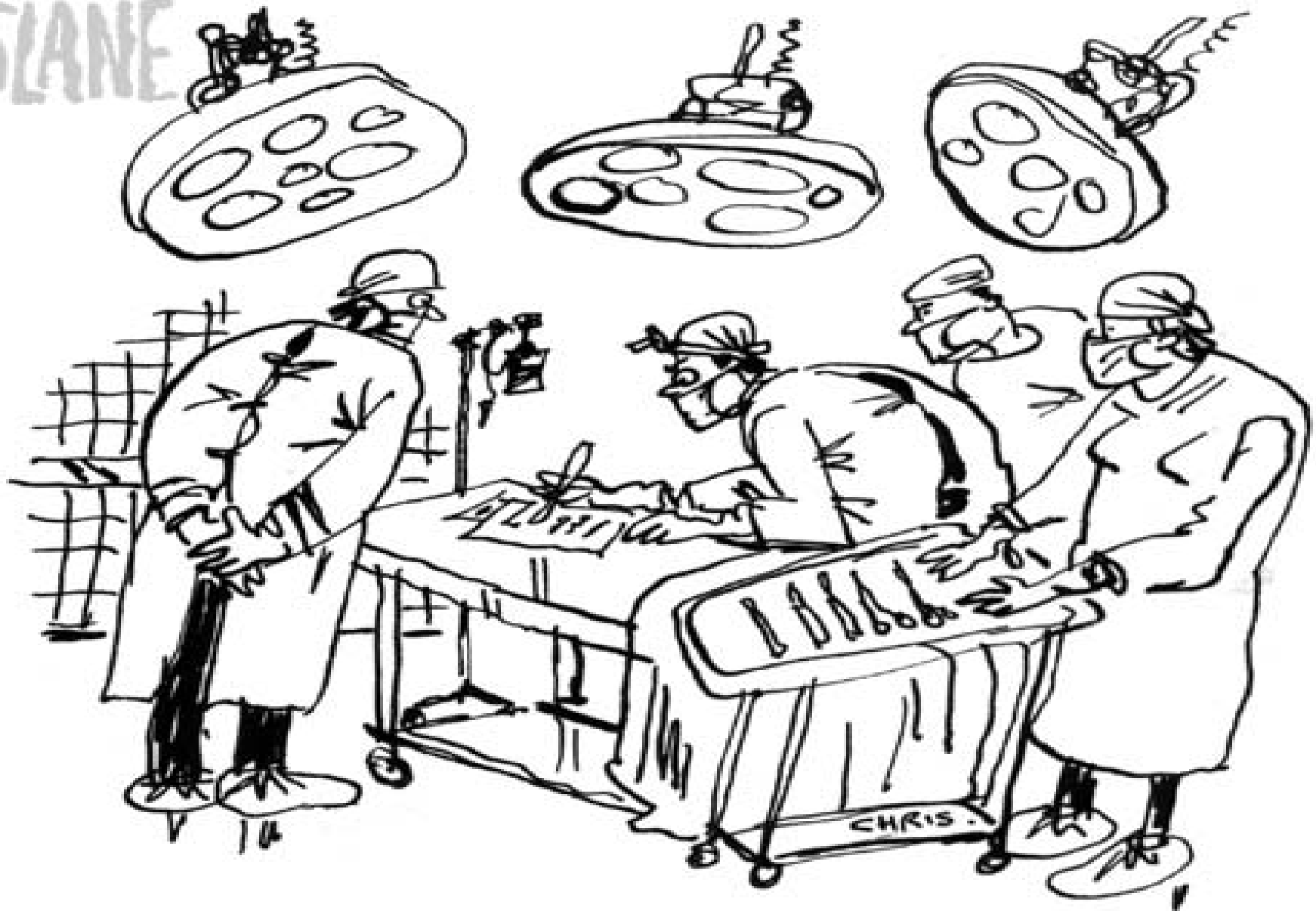
Information Custodian Responsibilities





Security, Privacy and Safety as Risk Issues

- *Security, privacy and safety are mandatory features of all SSHA products and services*
- *Not entirely compliance with legislation and standards issue*
- *Need to balance operational demands with real business risks*



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

Privacy

- *Managing compliance with multiple authorities (PHIPA, FIPPA, PIPEDA)*
- *Defining privacy responsibilities in a multi-organizational information sharing environment*
- *Reinventing the Privacy Impact Assessment*

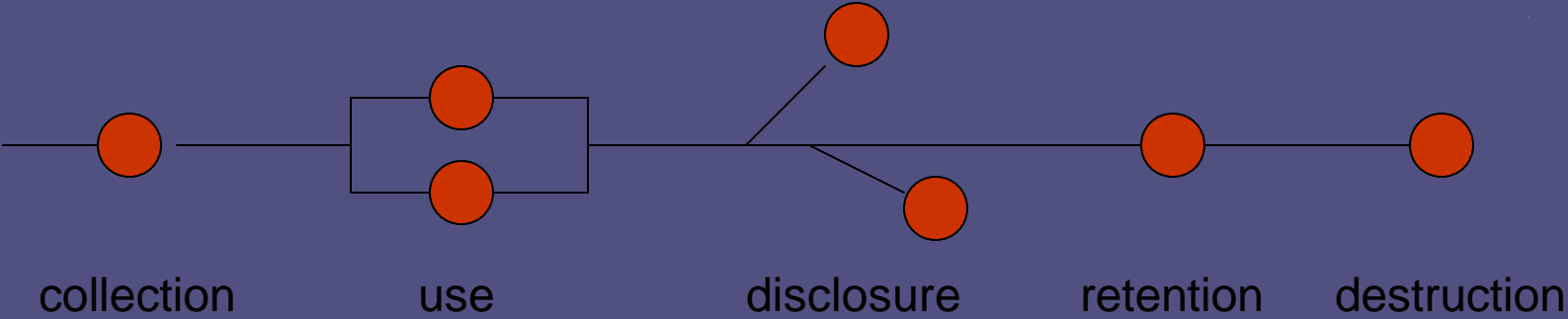
Privacy Impact Assessment

Project Description

Data Flow Analysis

Privacy Analysis/Risk Assessment

Recommendations



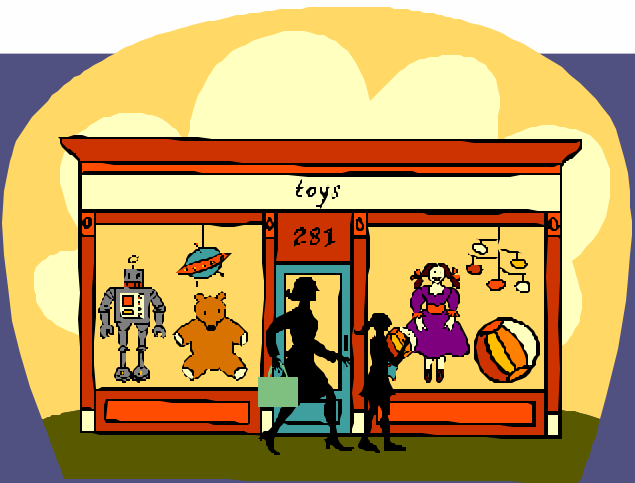


PSSST-WANNA BUY
SOME PERSONAL
INFORMATION?

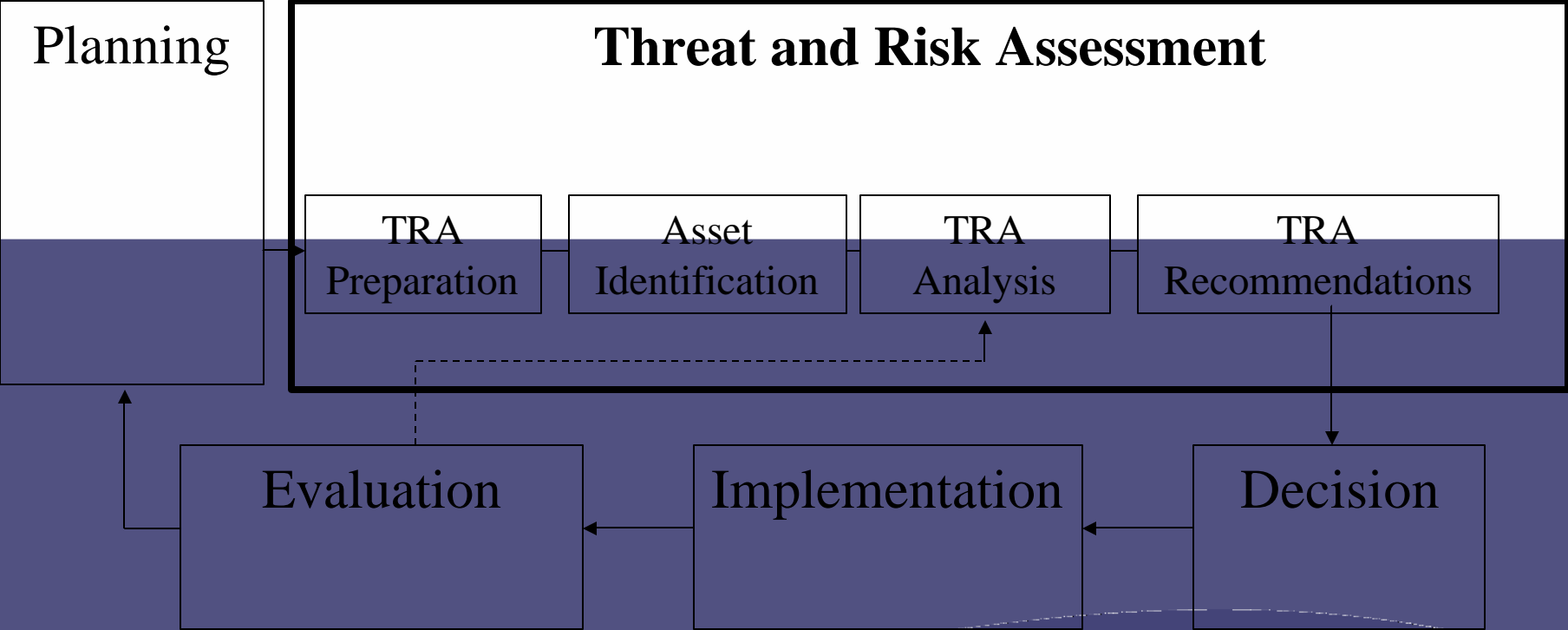
CHRIS.

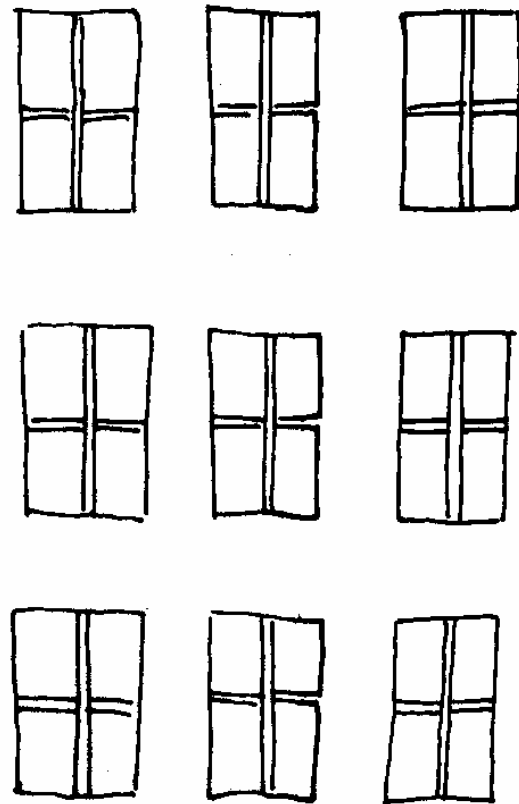
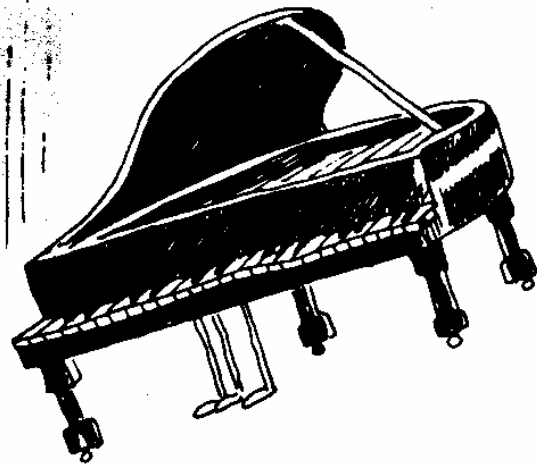
Security

- *Understanding the threat environment*
- *Identifying your assets – knowing what you have and who might want to steal, damage or compromise it*
- *More than confidentiality – addressing issues of availability and integrity*
- *Reinventing the Threat and Risk Assessment*



Threat and Risk Assessment





Larson

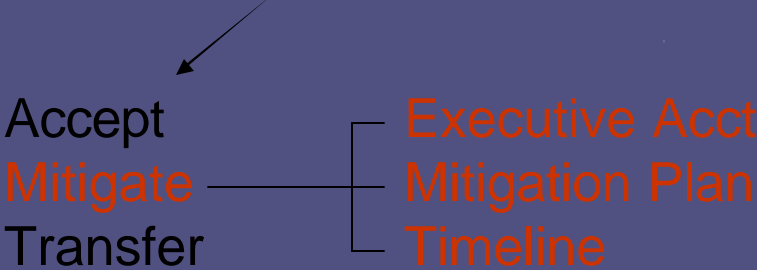
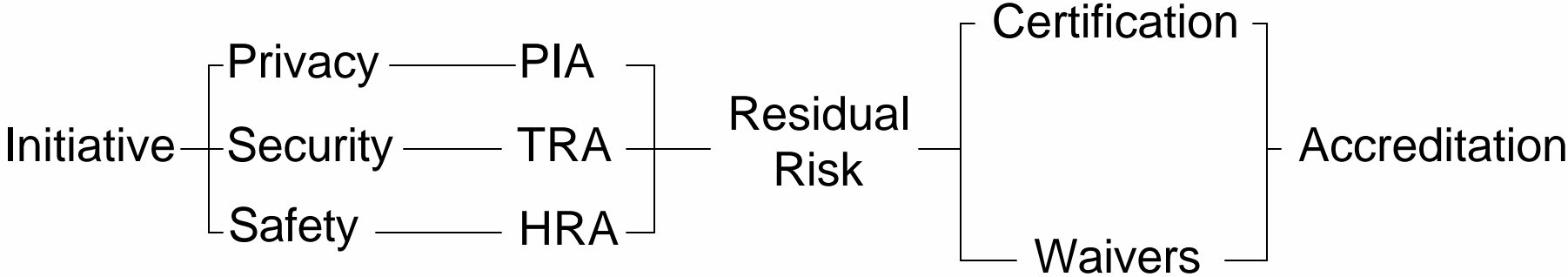
Safety

- ***Safety (or lack of it) – the silent killer***
- ***Currently not addressed in any organized form***
- ***Understanding the safety risks associated with health information systems***
- ***Pushing the envelope – establishing standards and methodologies for safety in health information systems***
- ***Hazard Risk Analysis***

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*

Certification and Accreditation



Importance of Standards

- *Avoid arbitrary or subjective measures of risk, need lock to legislative, national or international standards*
- *Standards used by SSHA for C&A*
 - Security – ISO 17799
 - Privacy – CSA Privacy Code, PHIPA, FIPPA, PIPEDA
 - Safety – Draft ISO Standard for HIS hazard classification

The Road Ahead – what you can expect

1. Connect
2. Register
3. Email
4. Directory
5. Other services: applications, portals, etc.

The Road Ahead – Integrated Implementation

- All healthcare providers will have
 - Connectivity
 - PC, Internet, SSHA network
 - Secure email
 - Directory
 - Emergency messages
 - Information - e.g. portals, applications
 - Appropriate registration
 - Privacy and Security training
 - Products and services training

Balancing Competing Demands – *Optimizing* Service Delivery, Privacy, Security and Safety



Your Questions

www.ssha.on.ca