



Privacy Briefing Workshop 1

A beginner's introduction to key privacy issues in Health – what you should know and how to act

Peter Croll and Bill Caelli

10 November 2008

OBJECTIVE

“The aim of this workshop is to give an overview of the most pertinent issues to consider when addressing Health Privacy with Information and Communication Technology (ICT). This non-technical introduction is geared towards participants from a wide range of backgrounds from both Health and ICT. It will cover the necessary groundwork required for developing a health privacy perspective that is both safe and sustainable with our emerging eHealth environments.”

CONTENTS:

- **A) Introduction to key privacy issues with Health systems:**
 - Introduction - what makes health privacy different?
 - Vulnerabilities, threats and countermeasures with advances in ICT
 - Where does health information go?
(Collecting, accessing, processing, transmitting, storing and managing health data)
 - Navigating the legal and regulatory jungle
 - Secondary use, fear and trust
- **B) Managing Health ICT privacy:**
 - Your responsibilities - breaches, notification, risk management, policies, etc.
 - Choosing the right systems - “look before you leap”
 - Education, training and staffing
 - Managing a sustainable vision with Health IT for the future

A) Introduction to key privacy issues with Health systems:

What makes health different?

- Complex legislation and policies
- Disparate systems, applications and methods
- Whole of population
- Limited choices for users and clinicians
- Consumer's expectations
- Ethical and human research issues
- Individual's moral rights
- Lives are at risk
- Breach damage is for life (non- reversible)
- ~~Nobody is interested in your health records!!~~

WRONG!

You are here: [LAT Home](#) > [California | Local](#)

California/Local

Columnists:

- » [Steve Lopez](#)
- » [Sandy Banks](#)
- » [Patt Morrison](#)
- » [George Skelton](#)
- » [Dana Parsons](#)
- » [Steve Harvey](#)
- » [Steve Hymon](#)

Community Papers:

- » [Burbank](#)
- » [Newport Beach](#)
- » [Laguna Beach](#)
- » [Huntington Beach](#)
- » [Glendale](#)

News/Opinion

- [California | Local](#)
- [National](#)
- [World](#)
- [Business](#)
- [Sports](#)
- [Campaign '08](#)
- [Science](#)
- [Environment](#)
- [Opinion](#)

Arts/Entertainment



Tally of improperly accessed UCLA patient records tops 1,000

As the state investigation ends, 1,041 people's records are found to have been subjected to snoops.

By Rong-Gong Lin II
October 30, 2008

The number of patients whose hospital records were improperly accessed by employees at the UCLA Hospital System has topped 1,000, state officials said Wednesday.

Kathleen Billingsley, director of the California Department of Public Health's Center for Healthcare Quality, said the records of 1,041 patients have been breached, up from 939 in the state's last report in August.



After livers, cash to UCLA

» [UCLA investigates reported sexual assaults](#)
» [Contact the reporter with your experiences](#)

The total number of UCLA workers who have been disciplined for breaching patient records now stands at 165, up from 127 since August.

Wednesday's report was the sixth issued by the California Department of Public Health after articles ran in The Times

this year about UCLA employees prying into the records of celebrities and prominent patients, including California First Lady Maria Shriver, actress Farrah Fawcett and singer Britney Spears.

[Email](#) | [Print](#) | [Text](#) | [RSS](#)

ADVERTISEMENT

Most Viewed

Most E-mailed

1. [Lakers, Andrew Bynum agree to four-year deal](#)
2. [Schwarzenegger stands with bipartisan coalition opposing Proposition 5](#)
3. [Girl, 11, killed in crash outside Glendale middle school](#)
4. [McCain, Palin demand L.A. Times release Obama video](#)
5. [5 students held in shooting plot at Big Bear High School](#)
6. [Owner of motor home where body was found is charged with murder](#)
7. [Gay married couples face legal limbo if Prop. 8 passes](#)
8. [Fatal advice to The Enforcer, 'Don't take any firearms'](#)
9. [Fitness buffs fight back after being muscled out of Santa Monica neighborhood](#)
10. [Police: NY teacher's husband choked his wife and dumped her body after an argument](#)

Sports Headlines

1. [Lakers, Andrew Bynum agree to four-year deal](#)
2. [Beckham to join AC Milan in early January](#)
3. [Ben Olson getting closer to return](#)
4. [Winless Washington may see foes tremble again](#)

JACKSONVILLE, Fla. – Twenty hospital workers – nurses, admissions workers and patient relations staff – lost their jobs this week, accused of breaking federal privacy rules by accessing the medical records of the Jaguars' Richard Collier.

20 Hospital Workers Fired for Viewing Collier's Medical Records

POSTED: 4:04 pm EDT October 31, 2008

JACKSONVILLE, Fla. -- Twenty hospital workers -- nurses, admissions workers and patient relations staff -- lost their jobs this week, accused of breaking federal privacy rules by accessing the medical records of the Jaguars' Richard Collier.

Two weeks after Collier -- who was shot 14 times -- was well enough to be discharged from Shands-Jacksonville Medical Center, 20 hospital employees were fired for violating Collier's medical privacy.

Collier was rushed to Shands Sept. 2 after a gunman walked up to Collier's SUV as he waited outside a Riverside apartment and opened fire.

E-MAIL NEWS ALERTS

Get breaking news and daily headlines.

Enter E-Mail Address

► Browse all e-mail newsletters

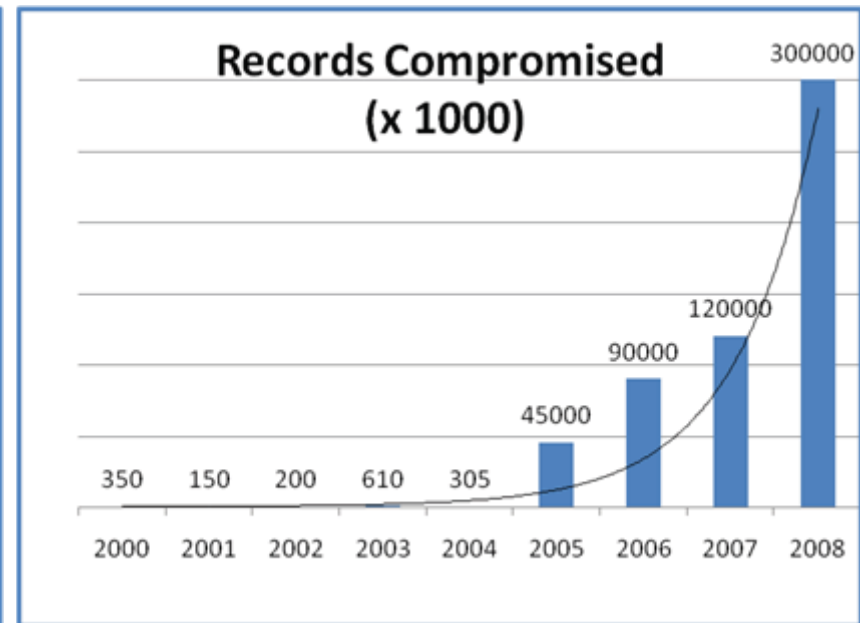
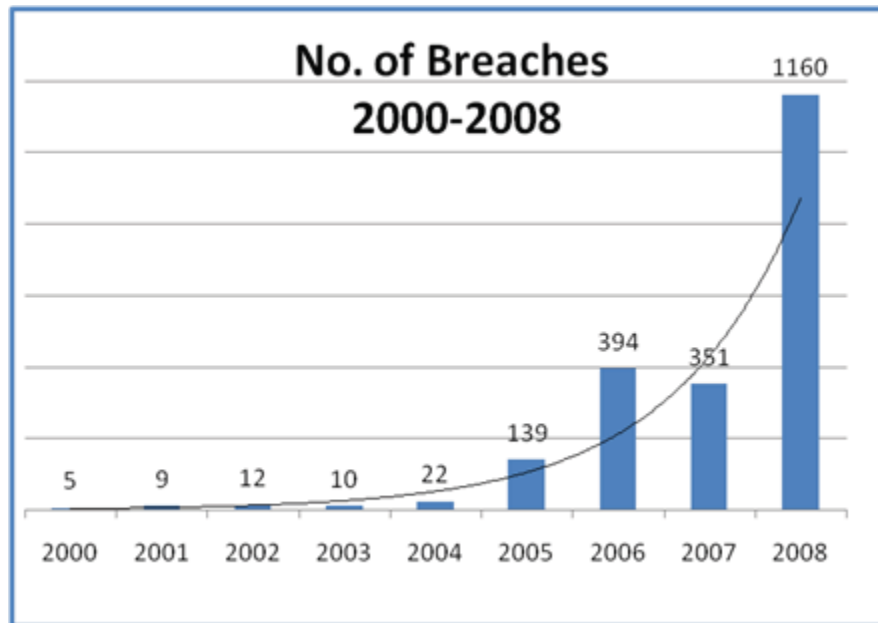
RELATED TO STORY

[+ Enlarge](#)



Breaches and Records compromised

- Consider the trends across all sectors:



a case of – not if but when?

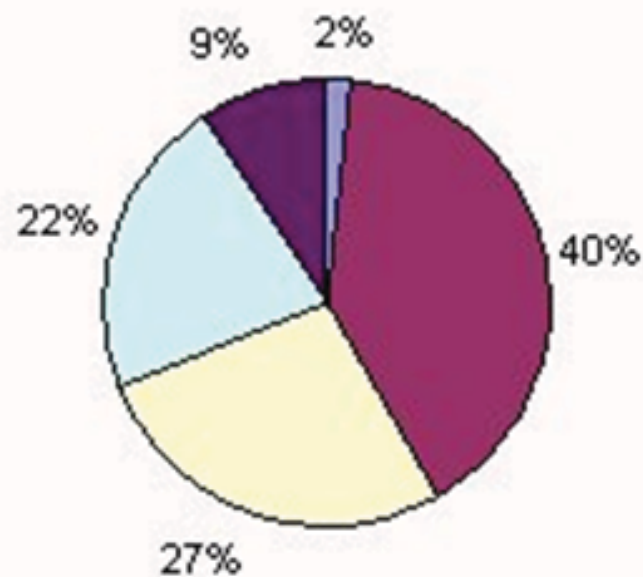
www.infosecurityanalysis.com

Healthcare / Medical

2000 - 2007

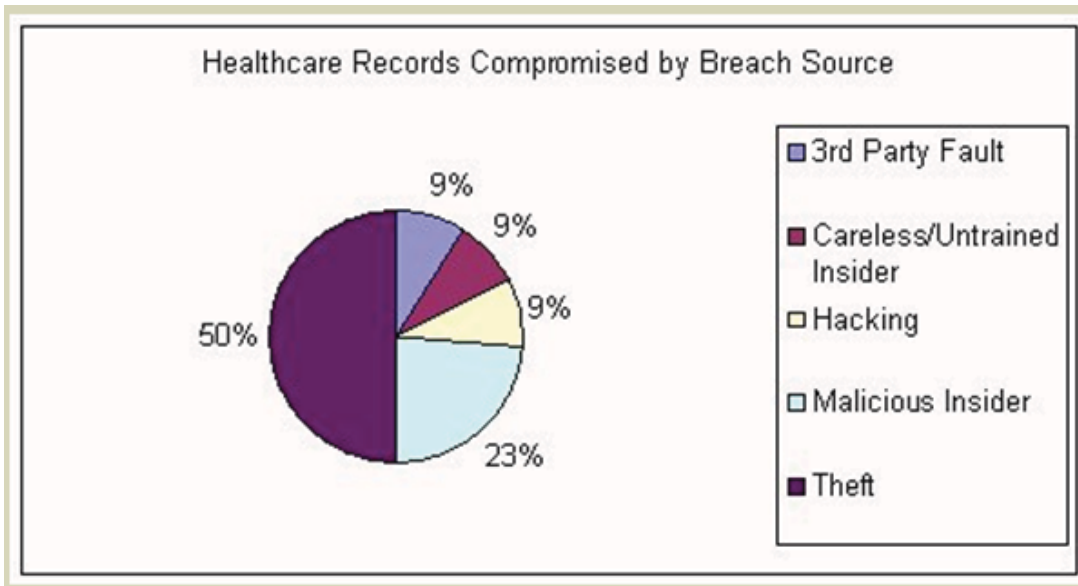
Breach Type

Healthcare Incidents by Breach Type



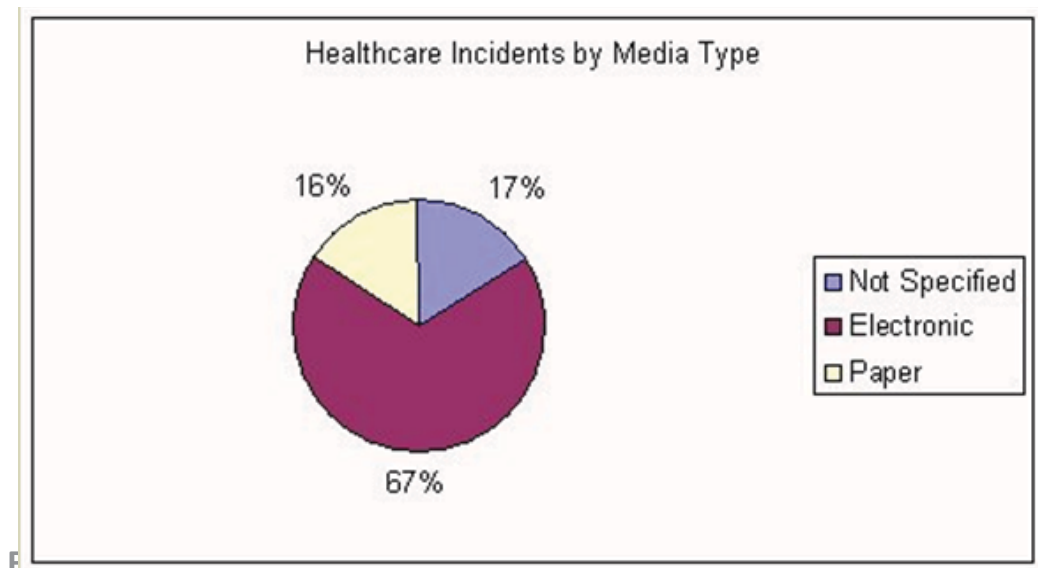
- Not Specified
- Data Breach
- Data Exposure
- Laptop
- Media Loss

Health Record Compromised – Who, What, Where?



Breach Source	Sum of Total Records
3rd Party Fault	475550
Careless/Untrained Insider	459392
Hacking	479726
Malicious Insider	1253050
Theft	2677133

Theft and Malicious insiders with Electronic records



19th June 2008

Jon Paul Oson, 38, of Chula Vista, California, was sentenced to 63 months behind bars and ordered to pay more than \$409,000 in restitution, according to federal prosecutors in San Diego. He was immediately taken into custody after the sentence was handed down on Monday. It is one of the stiffest penalties ever for a computer hacking offense.

*On December 23, Oson logged onto servers belonging to his former employer and disabled the program that automatically backed up **medical records for thousands of low-income patients**. Six days later, he logged on again, and in the span of 43 minutes, methodically deleted the files containing patients' appointment data, medical charts and other information.*

Personal Health Information Privacy

PHIPrivacy.net is brought to you by PogoWasRight.org

[HOME](#) [About](#) [Breaches](#) [Election '08](#) [Events](#) [Legislation](#) [Privacy Policy](#) [Resources](#) [RSS](#)

Nov-3-2008

Some ID-theft schemes target Canada's health-care system

Pauline Tam reports:

Criminals are exploiting lax security in government databases to assume false identities and take advantage of Canada's health-care system, warns a leading expert in identity fraud.

But such scams go largely unprosecuted because there is no concerted effort by government agencies to go after bogus health-care claimants, says former Edmonton police detective Joe Pendleton.

Pendleton, who helped uncover one of the country's most notorious identity-theft schemes, told an Ottawa conference of privacy experts Monday that existing federal and provincial privacy laws hamper criminal investigations by keeping even the most basic patient health records out of the reach of police.

Read more on [Canada.com](#)

Posted under [Non-U.S. breaches](#)

[Add comments](#)



subscribe

ARCHIVES

[November 2008](#)

[October 2008](#)

[September 2008](#)

[August 2008](#)

[July 2008](#)

[June 2008](#)

[May 2008](#)

[April 2008](#)

[March 2008](#)

[February 2008](#)

RECENT POSTS

[Some ID-theft schemes target Canada's health-care system](#)

[UK: Medical records found dumped near canal in Barrowford](#)

Nov-3-2008

UK: Medical records found dumped near canal in Barrowford

Simone Yates reports:

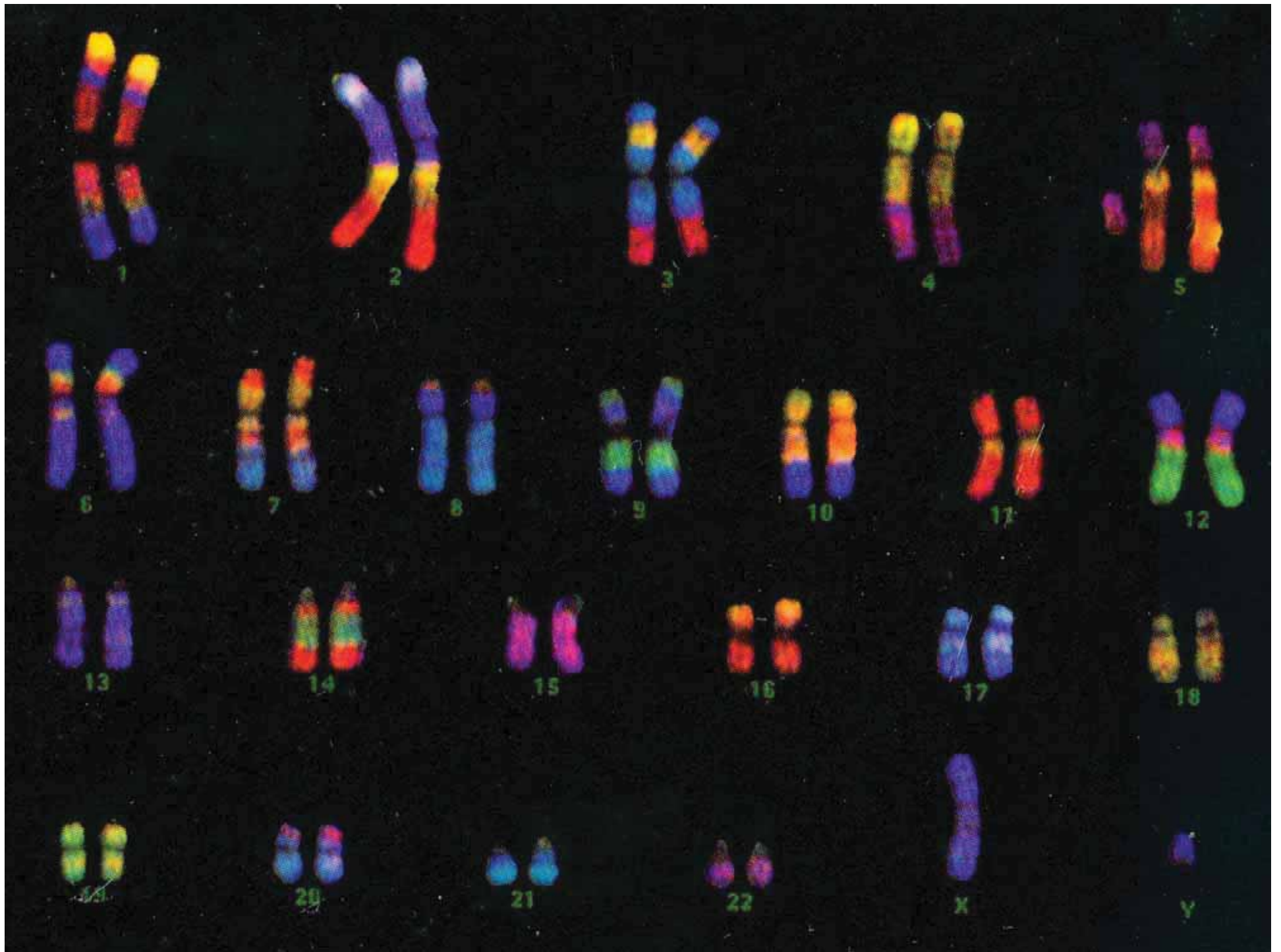
AN INVESTIGATION has been launched after hundreds of personal medical documents were found dumped beside a canal between Barrowford and Foulridge.



A) Introduction to key privacy issues with Health systems:

- Vulnerabilities, threats and countermeasures with advances in ICT

- ADVANCES IN ICT
- VULNERABILITIES, THREATS AND COUNTERMEASURES
- PRIVACY DEAD?



SPECIAL ISSUE: **WILL TECHNOLOGY KILL PRIVACY?**

SCIENTIFIC AMERICAN

Bug-Bots
and Other
**Spy
Gadgets**
page 70



September 2008

www.SciAm.com

THE FUTURE OF **PRIVACY**

Can we safeguard our information
in a high-tech, insecure world?

Internet-Age
Wiretapping

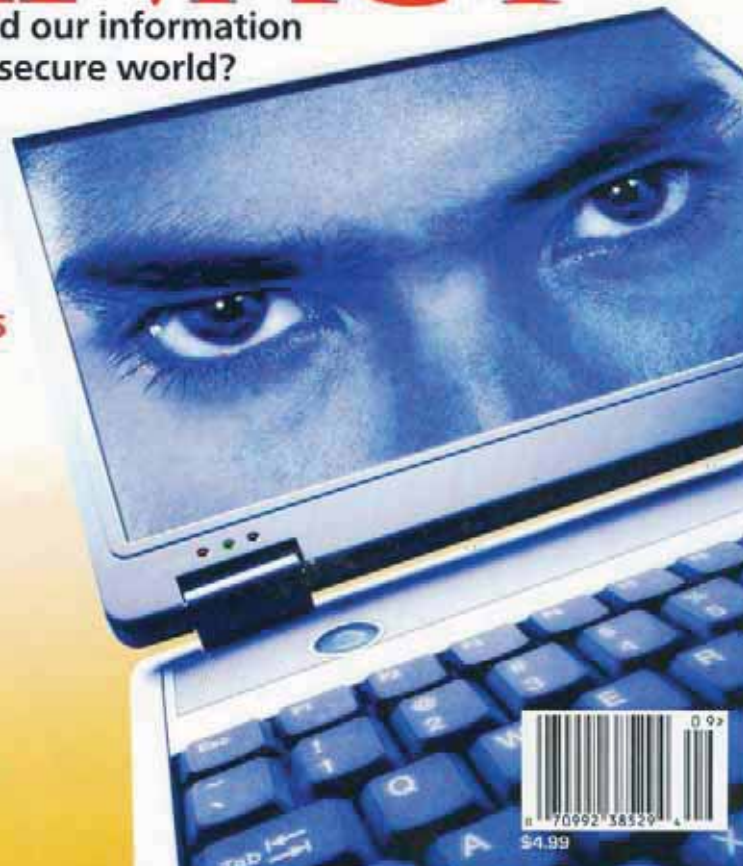
Cryptography for
Keeping Secrets

You Are Tagged:
RFID Chips

Beyond Fingerprints:
Biometric I.D.

Privacy in a
Facebook Age

Defending Genetic
Confidentiality



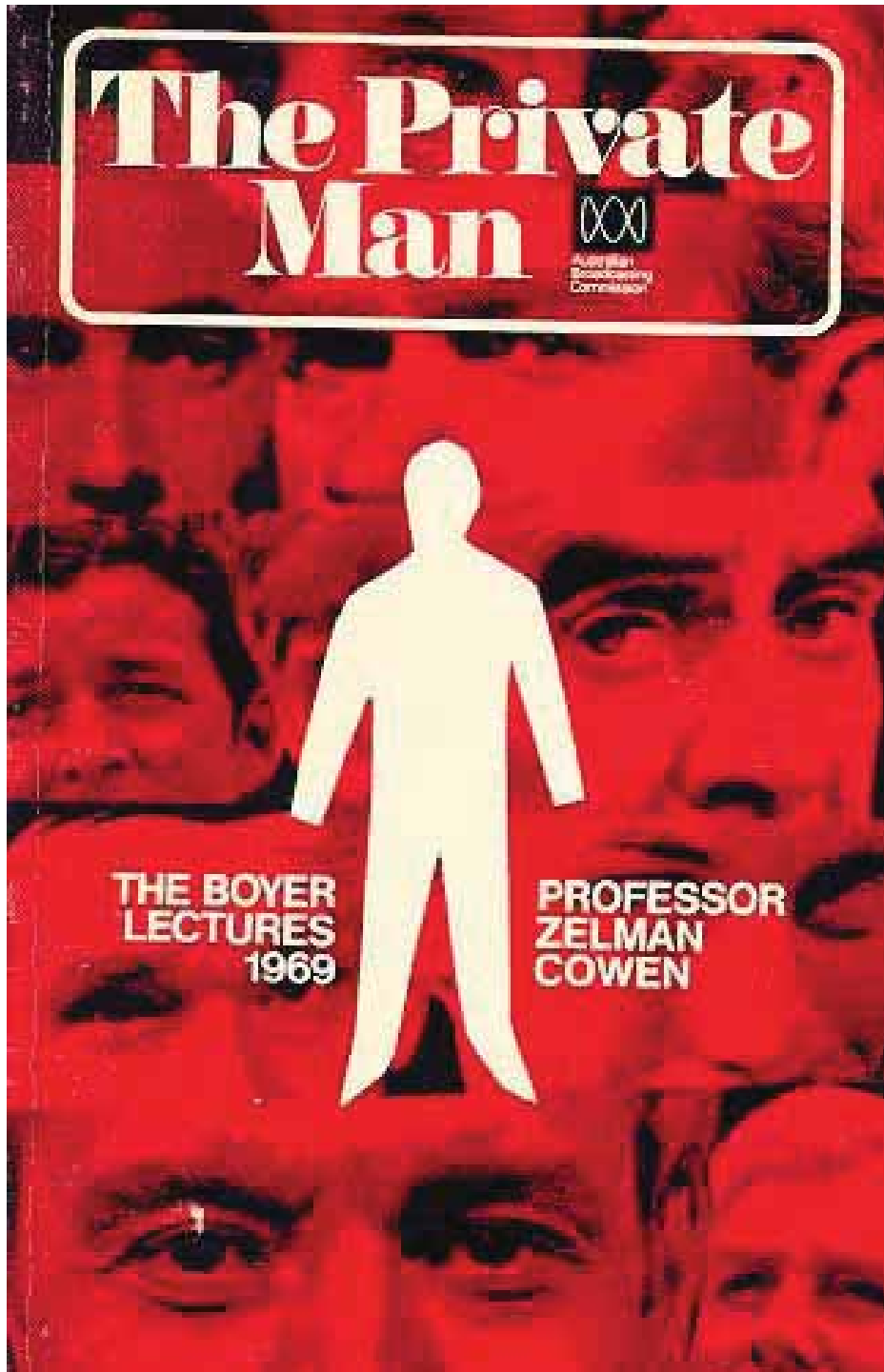
\$4.99

© 2008

IMPACT OF COMMODITY LEVEL ICT

Total convergence:

Computers
Telecommunications
Content
with
Global
Ubiquity



1969

- Early recognition
- ICT systems ARE different to paper “scale” at all levels
- Matter of “scale”

Sun on Privacy: 'Get Over It'

Polly Sprenger 01.26.99

The chief executive officer of Sun Microsystems said Monday that consumer privacy issues are a "red herring."

"You have zero privacy anyway," Scott McNealy told a group of reporters and analysts Monday night at an event to launch his company's new Jini technology.....

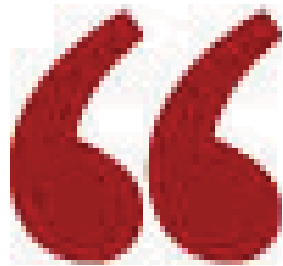
Get over it."

Computerworld, 27 Nov 2001:

"Like, 'You have no privacy, get over it.' I'm pretty famous for that one."

Sun Microsystems is a member of the [Online Privacy Alliance](#), an industry coalition that seeks to head off government regulation of online consumer privacy in favor of an industry self-regulation approach.





Privacy is dead. Get over it. You can't put the genie back in the bottle.

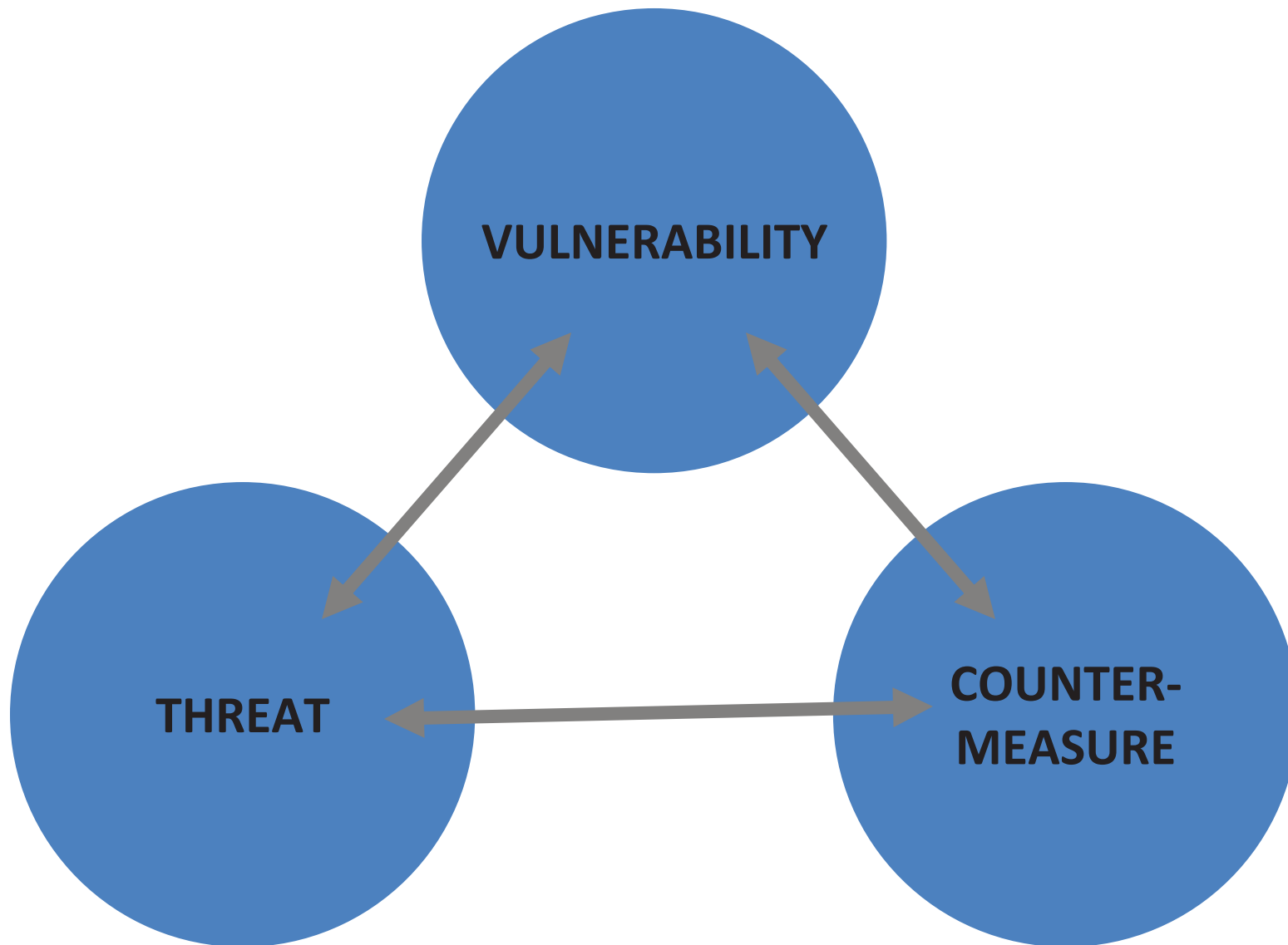
The Grill: Privacy is a thing of the past, says private investigator Private eye Steven Rambam explains what he does, how he knows everything about you and why he's not the one you should be worried about.

By Robert L. Mitchell - October 10, 2008



“Morris” Worm 2 November 1988

- 10% all Internet-connected systems – down!
- three years probation,
- ordered to pay \$10,000 fine
- perform 400 hours of community service
- violation of USA Federal
 - Computer Fraud and Abuse Act of 1986.

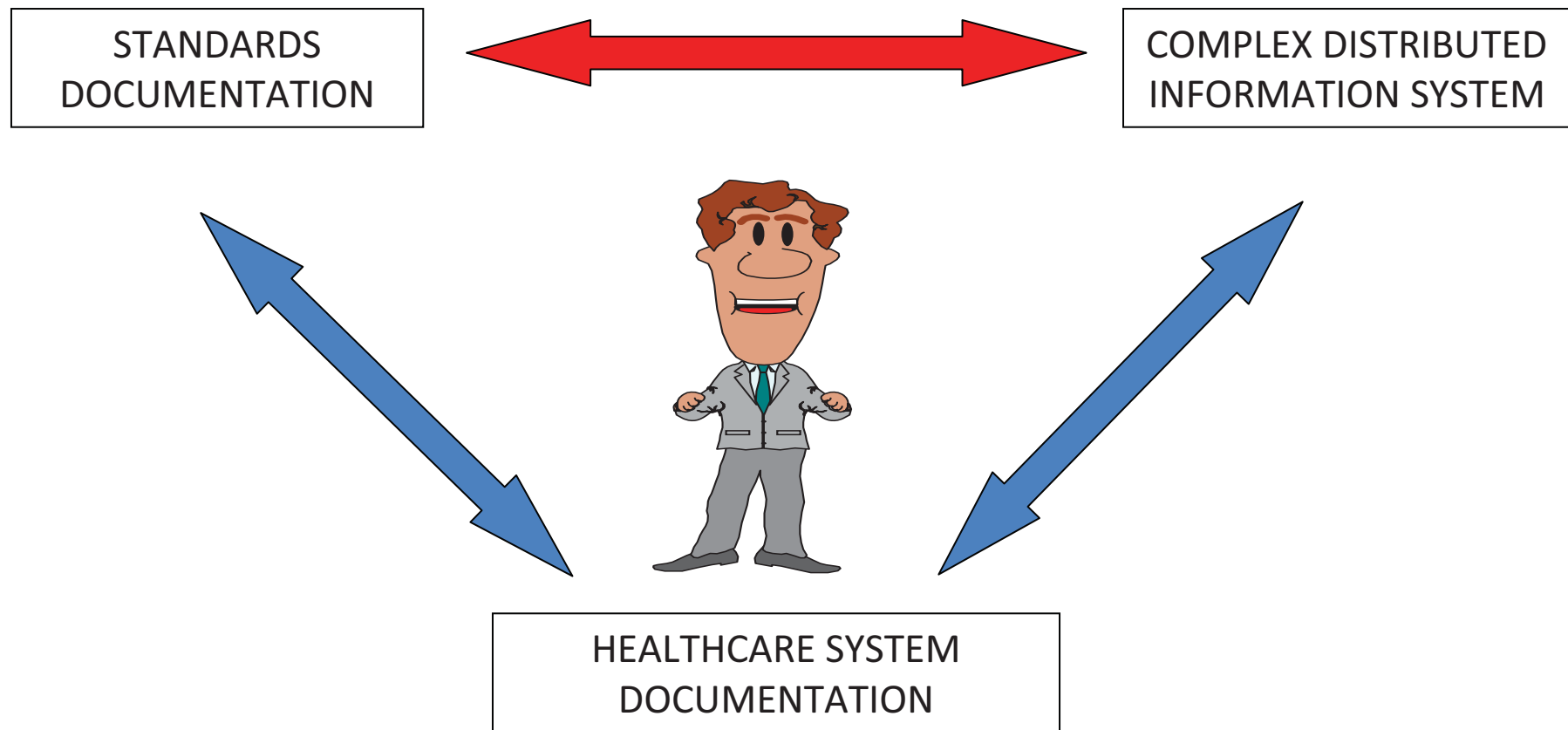


THREATS:

External & Internal

- Global connection
 - 24/7
 - Motivation
 - Healthcare
specifics!
 - Expertise
 - Ahead of us!
 - Organised vs
disorganised
- “Gen Y”
 - ICT literate
 - Mobile / personal
products
 - iPod / iPhone / USB
 - Motivation

COMPLIANCE CHECKING: THE REAL PROBLEM



A) Introduction to key privacy issues with Health systems:

Where does health information go?

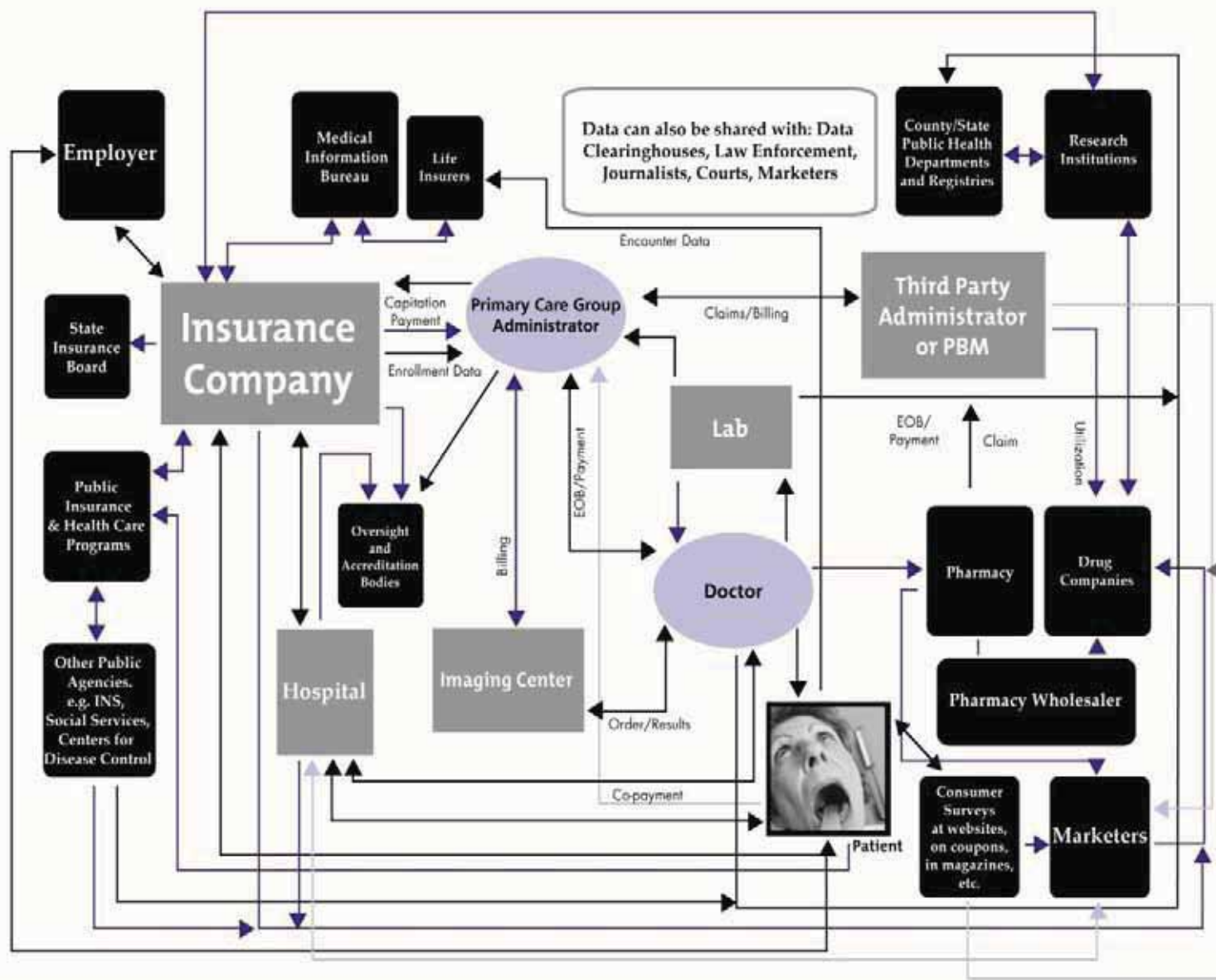
(Collecting, accessing, processing, transmitting, storing and managing health data)

- NPP's cover:
 - *Collection, Use and Disclosure, Access and Correction, Security, Transborder data flows, etc. (total 10)*
- IPP's cover:
 - *Manner/Purpose of Collection, Storage, Security, Access and Amendment, Use, Disclosure, etc. (total 11)*
- Proposed UPP's cover:
 - *Collection, Notification, Openness, Use and Disclosure, Data Security, Access and Correction, Cross-border data flows, etc. (11 proposed)*
- Privacy Impact Assessment (PIA)
 - *guides specify creating an Information Flow Map*

Do You Know Where Your Medical Information Goes?

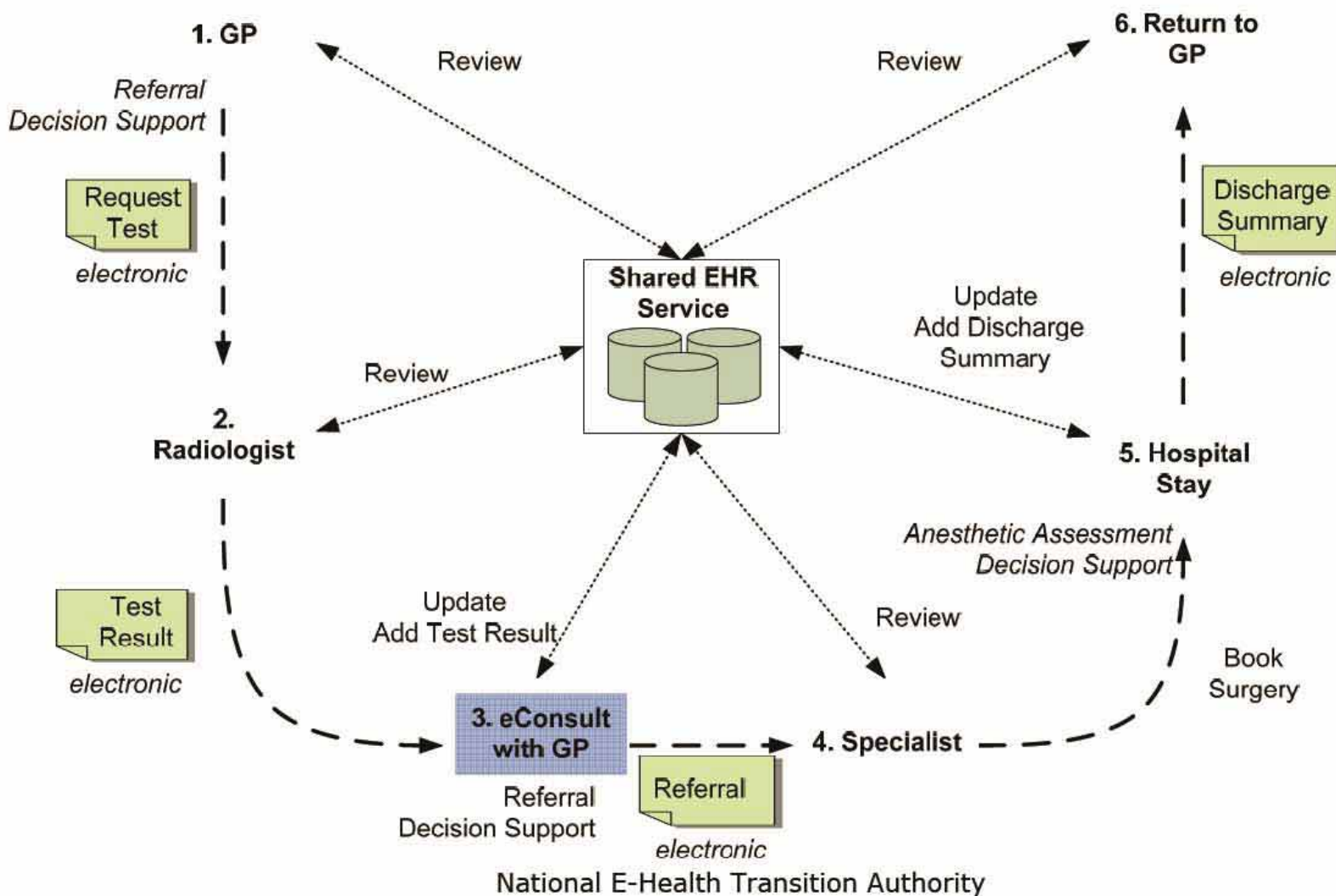
Sample Data Flow

Based on a presentation developed by the California HealthCare Foundation



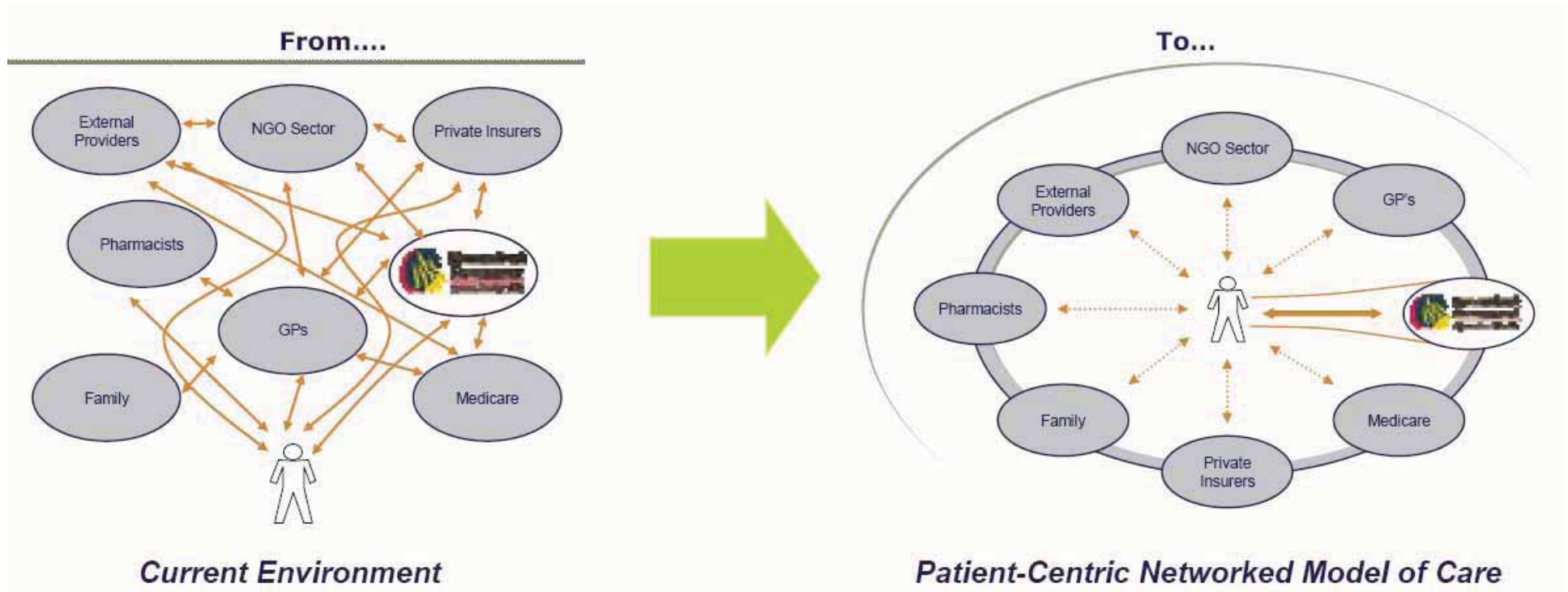
Please note that the explanations are meant to be illustrative. They are not comprehensive.

Shared EHR using (electronic) clinical processes



National E-Health Transition Authority

Queensland Health eHealth Strategy



A) Introduction to key privacy issues with Health systems: Navigating the legal and regulatory jungle

Commonwealth:

- Privacy Act 1988
 - ❑ handling of personal info by Cth & ACT public sector agencies;
 - ❑ handling of personal info by some private sector organisations
 - ❑ Part IIIA: credit worthiness info held by credit reporters & providers;
 - ❑ tax file number use by individuals & organisations;
- Taxation Administration Act 1953 (handling of tax file numbers)
- National Health Act 1953 (handling of Medicare and pharmaceutical benefits info)
- Data-matching Program (Assistance and Tax) Act 1990 (matching M/ATO & other assistance agencies)
- Freedom of Information Act 1982
- Archives Act 1983
- Crimes Act 1914, Pt VIII (spent convictions)
- Surveillance Devices Act 2004
- Telecommunications Act 1997 (personal info disclosed by telco providers)
- Telecommunications (Interception) Act 1979

Northern Territory:

- Information Act 2002 (privacy, FOI and public records)
- Criminal Records (Spent Convictions) Act 1992
- Surveillance Devices Act 2000
- Telecommunications (Interception) Northern Territory Act 2001 (not yet in force)

Western Australia:

- No privacy law not administrative privacy regime, but see discussion paper (released 20 May 2003) and note that privacy legislation is intended to be introduced, possibly before Christmas 2004.
- Freedom of Information Act 1992
- State Records Act 2000
- Spent Convictions Act 1988
- Surveillance Devices Act 1998
- Telecommunications (Interception) Western Australia Act 1996

South Australia:

- No privacy law, but see Cabinet Administrative instruction to comply with Information Privacy Principles (originally issued in 1989, re-issued in 1992), and note the SA Privacy Committee reports that a paper is being prepared for the Minister on the future of a privacy regime for SA.
- Freedom of Information Act 1991
- State Records Act 1997
- Criminal Law Consolidation Act 1935, Part 5A (identity theft)
- Listening and Surveillance Devices Act 1972
- Telecommunications (Interception) Act 1988
- No spent convictions law, but see discussion paper (released 5 May 2004)

Queensland:

- No privacy law, but see State Government Standards Nos. 42 (Information Privacy, Sep 2001) & 42A (Information Privacy for the Old Dept of Health, Sep 2001) (administrative standards); and the Government commitment to review the privacy standards after 2 years to determine the need for privacy legislation; also see Parliamentary report (tabled April 1998) and the then Government response (tabled 21 October 1998)
- Freedom of Information Act 1992
- Public Records Act 2002
- Criminal Law (Rehabilitation of Offenders) Act 1986 (spent convictions)
- Invasion of Privacy Act 1971 (credit reporting, listening devices, invasion of privacy of the home)
- Police Powers and Responsibilities Act 2000, Chap 4 (covert evidence gathering)
- No state telecommunications interception power, but see Parliamentary report (tabled December 1999) and the then Government interim response (tabled 1 November 2000)

New South Wales:

- Privacy and Personal Information Protection Act 1998
- Health Records and Information Privacy Act 2002
- Freedom of Information Act 1989
- State Records Act 1998
- Criminal Records Act 1991 (spent convictions)
- Listening Devices Act 1984
- Workplace Values Surveillance Act 1998, to be repealed by Workplace Surveillance Act 2005 (not yet in force)
- Telecommunications (Interception) (New South Wales) Act 1987

Australian Capital Territory:

- Privacy Act 1988 (Cth)
- Health Records (Privacy and Access) Act 1997
- Freedom of Information Act 1989
- Territory Records Act 2002 (public records)
- Human Rights Act 2004 (right to privacy)
- Spent Convictions Act 2000
- Listening Devices Act 1982

Victoria:

- Information Privacy Act 2000
- Health Records Act 2001
- Freedom of Information Act 1982
- Public Records Act 1973
- No spent convictions law, but see Victoria Police policy on release of criminal history information
- Surveillance Devices Act 1999
- Telecommunications (Interception) (State Provisions) Act 1988

Tasmania:

- Personal Information Protection Act 2004
- Freedom of Information Act 1991
- Archives Act 1983
- Amalgamated Convictions Act 2002 (spent convictions)
- Listening Devices Act 1991
- Telecommunications (Interception) Tasmania Act 1999

Privacy and Related Legislation in Australia

What Legislation Applies to Privacy?

- **Federal privacy legislation may apply**
- **State legislation may apply (not all states, e.g. WA, SA)**
 - Health Records and Information Privacy Act 2002 (NSW), Information Privacy Act 2000 (Vic), Information Standard 42, Section 62A of Part 7 of the Health Services Act 1991 (QLD), The Personal Information and Protection Act 2004 (Tas), Information Act 2002 (NT).
- **Only when an individual can be reasonably identified –**
 - Personal Information is any form of information about an individual whose identity is apparent or can be reasonably ascertained.
- **When you are a private company and a healthcare provider Privacy Amendment (Private Sector) Act 2000**
- **exclusions - refer to NHRMA (guidelines under section 95A)**

*Beware administratively based guidelines e.g. IS42A: Information Standard No. 42A (information Privacy Guidelines for Qld Health) aim to guide in situations where legislation does not specifically cover.

What are you required by law to do?

- Follow the 11 Information Privacy Principles (IPPs) that apply to Australian Government and ACT Government agencies
- and 10 National Privacy Principles (NPPs) that apply in the private sector
- Follow state legislation (where applicable)
- Take care - some overlap and some contradict
- Distinguish between
 - Personal information: “information or an opinion....about an individual whose identity is apparent.”
 - and Sensitive information (Health) which includes any information collected during the course of providing treatment and care to an individual

The NPPs and Health Information

- Provides a higher level of protection
- Information may be used or disclosed only for the purpose it was collected
- OR a directly related secondary purpose
 - and only so long as the health consumer would 'reasonably' expect the information to be used in this way.
- Special provision:
 - the disclosure of health information to an individual's family member or guardian where the individual is physically or legally unable to consent to disclosure;
 - the use of health information in medical research relevant to public health or safety;
 - the use of health information in the compilation and analysis of statistics relevant to public health and safety; and
 - the use of health information in the management, funding or monitoring of a health service.

Data Collection: With or Without consent?

- The NPPs acknowledge public interest in allowing the use of health information in the management activities of health service providers and researchers **without consent** in limited circumstances for:
 - research relevant to public health or public safety;
 - the compilation or analysis of statistics relevant to public health or public safety;
 - the management, funding or monitoring of a health service.
- But only:
 - if it could not use de-identified information to achieve its purpose;
 - it is impracticable for the organisation to seek the consent of all the individuals involved
 - this depends on the scope of the data collection

Data Collection:

- It must be collected:
 - as required by law;
 - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;
 - in accordance with guidelines approved by the Privacy Commissioner under s 95A of the Privacy Act 1988.
- Patients/clients must be made reasonably aware of how their information will be collected and used including data which is not specifically consented and is routinely collected i.e. for service monitoring (risk mitigation)

Data Collection:

- Data collected for a consented specific purpose (e.g. a clinical trial) may still be available for reuse for a different purpose subject to appropriate ethical clearance.
- In privacy regimes '*disclosure*' normally refers to the transfer or release of information outside an organisation.
- However, for duty of confidentiality purposes with public health organisations (e.g. Qld Health) disclosure includes transference of information to ANY other person including other staff.

Note that: as soon as data is accessed from the medical record, where it was recorded for the specific purpose to support the clinical care of the patient, by other staff for a purpose other than the clinical care of the patient, it is being reused/disclosed. Further passing that information on again to another person for another purpose constitutes further disclosure

Service Management/ Quality Assurance/ Research?

- Often difficult to distinguish quality assurance activities in the health care context from research or service management/monitoring
- Service management includes service financial planning, service outcomes monitoring, Clinical Audit and possibly data mining of clinical databases
- Quality Assurance includes benchmarking and clinical improvement processes and possibly data mining
- For activities which amount to research or go on to publication then proceed
 - in accordance with the Section 95A Guidelines,
 - according to state legislation where applicable
 - subject to review by a Human Research Ethics Committee (HREC).

Information Privacy Principles under the Privacy Act 1988

- 1 - Manner and purpose of collection of personal information
- 2 - Solicitation of personal information from individual concerned
- 3 - Solicitation of personal information generally
- 4 - Storage and security of personal information
- 5 - Information relating to records kept by record-keeper
- 6 - Access to records containing personal information
- 7 - Alteration of records containing personal information
- 8 - Record-keeper to check accuracy etc of personal information before use
- 9 - Personal information to be used only for relevant purposes
- 10 - Limits on use of personal information
- 11 - Limits on disclosure of personal information

National Privacy Principles

- 1 - Collection
- 2 - Use and disclosure
- 3 - Data quality
- 4 - Data security
- 5 - Openness
- 6 - Access and correction
- 7 - Identifiers
- 8 - Anonymity
- 9 - Transborder data flows
- 10 - Sensitive information

A) Introduction to key privacy issues with Health systems:

Secondary use, fear and trust

- A UK report published Jan 06 by the **Academy of Medical Sciences** said that large population-scale medical studies are in jeopardy because of an "**undue emphasis on privacy**" by regulators.

- The inability to access medical data:

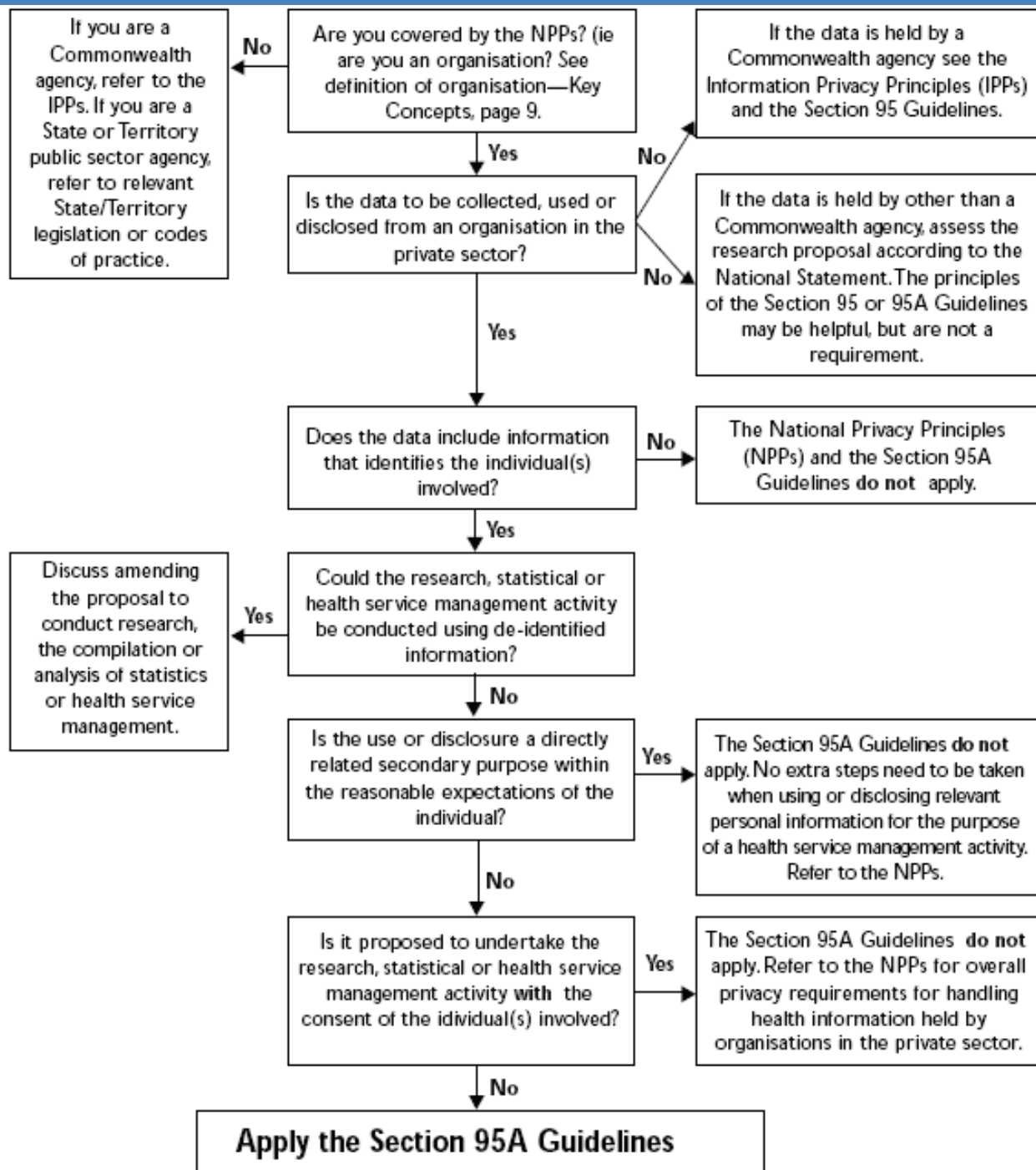
“There is no question that research is now at risk. Researchers are finding it increasingly difficult to get past the regulatory interpretation to allow their research to take place”

“and this is a detriment to public health.”

– Robert Souhami, cancer research, UCL

“Protecting health information privacy in research: how much law do Australians need?” MJA – Medicine and the Law (Volume 183, Number 6) 19 Sept05

PR Croll, “Are undue Privacy concerns putting our Health Research at high risk?” Privacy Law Bulletin, LexisNexis Butterworths, vol. 2, no.10, Apr 06, pp139-140.



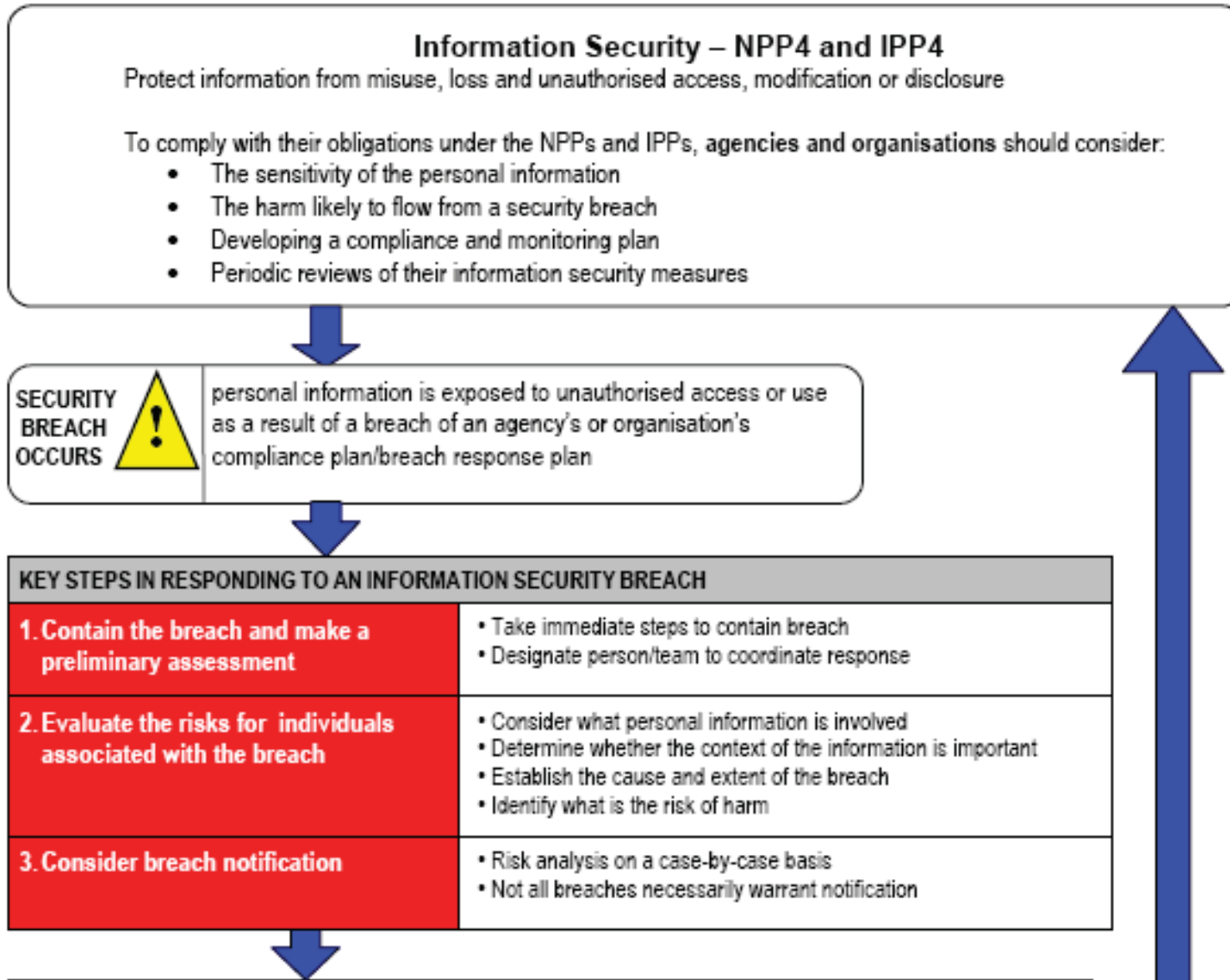
B) Managing Health ICT privacy:

Your responsibilities - breaches, notification, risk management, policies, etc.

- **There are four key steps to consider when responding to a breach or suspected breach:**
 - **Step 1: Contain the breach and do a preliminary assessment**
 - **Step 2: Evaluate the risks associated with the breach**
 - **Step 3: Consider notification**
 - **Step 4: Prevent future breaches**

- **Notification?**
 - “when there is a real risk of serious harm”
(identity harm, humiliation, reputation, physical harm, employment / financial loss)

Schematic guide to breach notification



Should affected individuals be notified?

<p>Where there is a real risk of serious harm, notification may enable individuals to take steps to avoid or mitigate harm. Consider:</p> <ul style="list-style-type: none"> • legal / contractual obligations to notify • risk of harm to individuals (identity crime; physical harm; humiliation; damage to reputation; loss of business or employment opportunities) 	<p>Process of notification</p> <ul style="list-style-type: none"> • When: as soon as possible • How: direct contact preferred (mail/phone) • Who: entity with the direct relationship with the affected individual • What: description of breach; type of personal information involved; steps to help mitigate; contact details for information and assistance
---	--

Should others be notified?

- Office of the Privacy Commissioner
- Police / Law Enforcement
- Professional or Regulatory Bodies
- Other agencies or organisations affected by the breach or contractually required to notify

4. Review the incident & take action to prevent future breaches

- Fully investigate the cause of the breach
- Consider developing a prevention plan
- Option of audit to ensure plan implemented

- Update security/ response plan
- Make appropriate changes to policies and procedures
- Revise staff training practices

B) Managing Health ICT privacy:

Choosing the right systems – “look before you leap”

- Cultural contrast – Europe and USA
- Grand Challenges
- Large Scale Systems in Healthcare
- Protection Policy Considerations
- The Data Centre



Europeans... tight and highly restricted privacy, preventing organizations from divulging information..

North Americans... less concerned about the commercial use of personal information, though much more concerned about government use.

The contrasting approaches reflect different cultures and histories.

COMPUTERS COME FROM THE USA



PRIVACY - VIEW - USA

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

The “right” to be “let alone”.

Samuel Warren and Louis Brandeis,
The Right to Privacy, 4 Harvard L.R. 193 (1890)



- USA constitutional history – “*Bill of Rights*”
- “*right*” as a fundamental concept
- Legislation – to provide remedies for **violation** of rights



*Personal **privacy** and national security in the 21st century both depend on protecting a set of systems that didn't even exist until late in the 20th — the electronic web of information-sharing known as cyberspace.*



Better Life ICT © 2008



CRA “Grand Challenges”

Workshop – Nov. 2003



Challenge #1:

Eliminate epidemic style attacks within 10 years;

Challenge #2:

*Develop tools and principles that allow construction of large scale systems for important societal applications that are highly **trustworthy** despite being attractive targets;*

Challenge #3:

Within 10 years, quantitative information systems risk management is at least as good as quantitative financial risk management; and

Challenge #4:

*For the dynamic, pervasive computing environments of the future, give user security they can understand and **privacy they can control.***

2003

1970: *“Report of the Defense Science Board Task Force on Computer Security”*

“The issue of providing security controls in computer systems will transcend the [US] Department of Defense. Furthermore, the computing industry will eventually have to supply computers and systems with appropriate safeguards”

“Thirty four years later, it is clear that the computing industry did not fulfill this prediction.”

Julie J C H Ryan & Corey D Schou

“On Security Education, Training and Certification”

Information Systems Control Journal, Vol 6, 2004

LARGE SCALE SYSTEMS IN HEALTHCARE

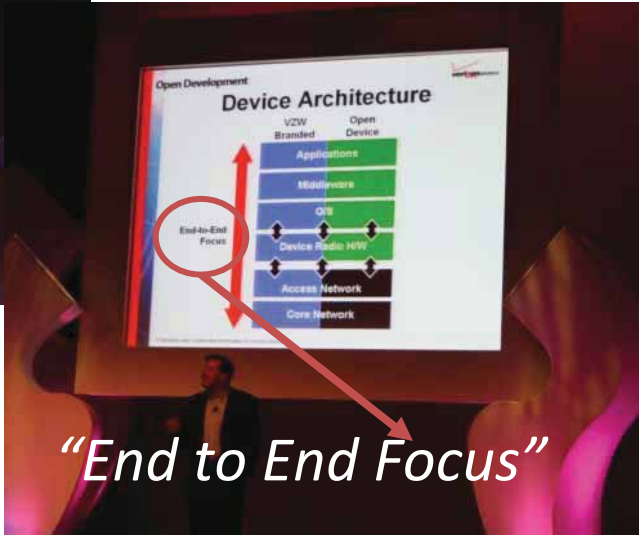
- systems catering for >10,000 “seats”
- of critical importance to their “owner/owners”
- of critical importance to their “audience”
- of national infrastructure importance
- public or private sector
- single or multiple management responsibility
- normally subject to some legislation/regulation
- transaction orientation
- Petabyte (1,000 terabyte) stores
 - (and beyond)



**CHOICE:
MOBILITY**



19 March 2008
Open Development
Device Conference



“End to End Focus”



- End of “Network Perimeter” as security enforcement entity
- Application / process / OS / Middleware / database focus



- USA / US States / UK
 - States: “*mandatory*” encryption of personal data
- USA Federal Trade Commission
 - crypto = reasonable
- UK – Data Commissioner
- Marks & Spencer: *“Ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part I of the Act and, in particular, ensure that the process of laptop hard drive encryption commenced by the data controller in October 2007 is completed by 1st April 2008”*

- **Recognition of infosec “market failure”**
 - over long time
 - ICT industry opposition to regulation
 - experienced in other industries / areas
 - cars, air transport, pharmaceuticals....etc.
- **New Legislative Models**
 - Australia
 - “*Motor Vehicle Standards Act*” 1989
 - broad legal imperatives
 - industry defined standards – enforced
 - ... with “*teeth*”.



BACK TO THE FUTURE - THE DATA CENTRE

- “Jurassic Park”
 - “rebirth” of the mainframe
- “Green IT”
 - lowering costs – increasing services
 - virtualisation
- “data at rest” – central responsibility
 - security
 - management
 - backup & recovery
 - legislation / regulation – growing!
- IT professionals – education/training
 - Outsourcing.



BACK TO THE FUTURE - THE DATA CENTRE



- “hardening” the data/server centre
 - “Common Criteria” – a choice measure
 - Some current examples:
 - SUN Solaris 10
 - IBM System z
 - Secure Linux
 - (Red Hat Enterprise Linux 5)
- Beyond commodity systems

**NETWORK PERIMETER SECURITY
NOW OBSOLETE**

BACK TO THE FUTURE - CHOICES: THE DATA CENTRE

- PC / desktop revolution
 - Workstation computing
- Real-world needs
 - Government, health, banking/finance, etc
 - “*Thinner*”, low-cost clients
 - Effective security management
 - simpler / centralised / controlled
 - audit / forensics
 - legislative / regulatory environment
- New choices / lower costs / lower power!

CHOOSING THE RIGHT SYSTEM / SERVICE

SUMMARY:

- Beyond the network
- Data repository
- Data in collection, transmission, processing, storage
- Reliability & Availability
- Backup & Recovery

- Beyond the commodity system
- Home PC is NOT a healthcare data system
- Other industry choices exist
- Enforcing policy & legislation

SUMMARY:

ICT INDUSTRY (PRODUCTS & SERVICES):

LEAST REGULATED

LEAST UNDERSTOOD

SUMMARY:

**ALL COMPUTERS AND SYSTEMS
ARE NOT THE SAME FROM A
PRIVACY ENFORCEMENT
(CONFIDENTIALITY) VIEWPOINT**

B) Managing Health ICT privacy:

Education, training and staffing

- What's in a word?
- Human rights
- Outsourcing & offshoring
- Governance & Compliance
- Technology
- ICT Education Crisis

WORDS

Security

Confidentiality

confidential

confidential quality; state of being

1. confident, bold
2. of the nature of confidence; spoken or written in confidence; characterized by the communication of secrets or **private** matters

Integrity

Availability

Privacy

the state or quality of being **private**

- 1.a the state or condition of being withdrawn from the society of others
- 1.b The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion

Safety

Oxford English Dictionary, Oxford University Press 2002.

GERMANY

Sicherheit

security
safety”

Zuruckgezogenheit

privacy

- Meaning of words – varies by language & culture
- Often no easy translation
- Meaning based on context

Langenscheidt's Concise German Dictionary, Messinger & Rudenberg - 1964/67

Article 12

*No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Universal Declaration of Human Rights (UDHR)

United Nations General Assembly

(10 December 1948

Palais de Chaillot, Paris).



EDUCATION, TRAINING & STAFFING - OPTIONS & CHOICES

- **Outsourcing & offshoring**
- Contract specification & mgmt
- Understanding the outsourcer
- Extra-territorial legal limitations
- Your own responsibilities

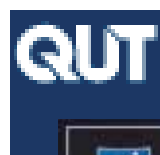
- **Governance & Compliance**
 - Australian legal & regulatory regime
 - Federal / State / Local
 - Enterprise policy

- **Technology**
 - Knowing & understanding the choices
 - Hardware / software / networks
 - System & application levels



EDUCATION, TRAINING & STAFFING - OPTIONS & CHOICES

- Academic vs Industry
- Education vs Training
- **Industry training & certification**
 - Vendor neutral vs Vendor specific
 - Activity specific (*“ethical hacking”*, etc.)
 - Product specific
 - Support vs Specification / development



ISC² (CISSP)
ISACA (CISM)
Sans Institute
iapp
.....

ICT EDUCATION CRISIS

ICT SKILLS GAP

*CSU senior lecturer in computing Martin Hale said the IT industry was facing a crisis, **with a 66 per cent fall in IT enrolments since 2002.***

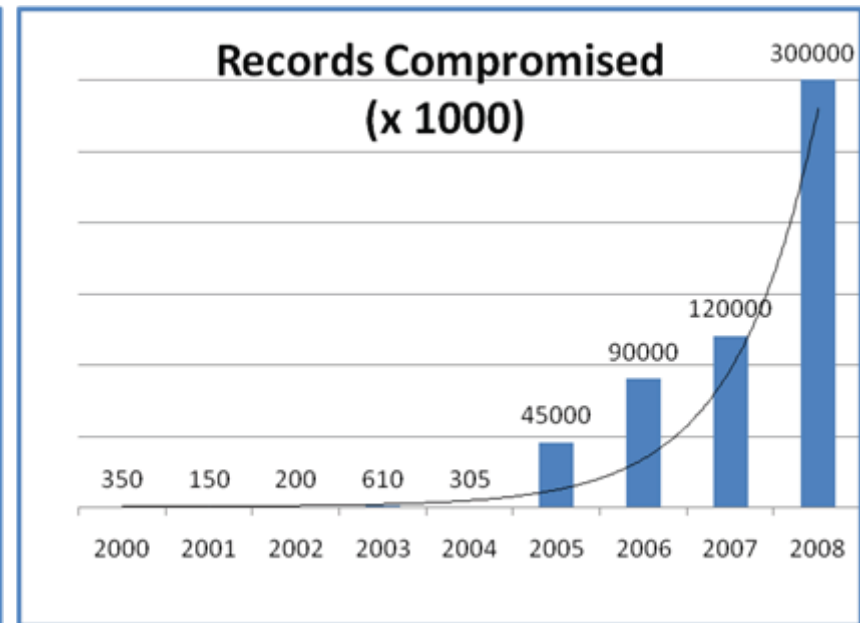
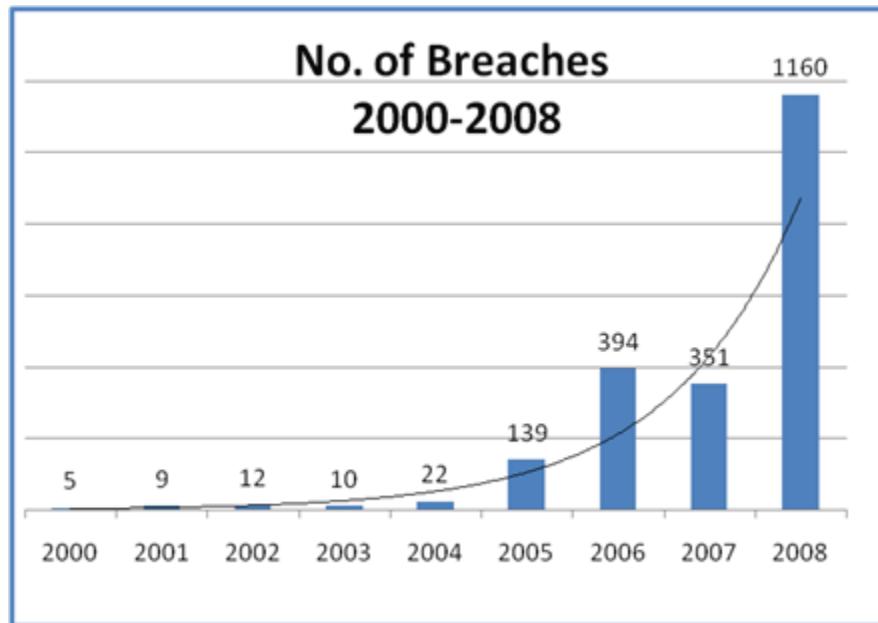
*Yet more than 100,000 IT positions had been created in that time. **“There is a very frightening skills shortage in the IT industry and it’s something CEOs need to know about,”** he said.*

B) Managing Health ICT privacy:
**Managing a sustainable vision
with Health IT for the future**

- When will the exponential expansion of breaches stop?
- What is your plan for Self-Assessment?
- When to undertake a Privacy Impact Assessment and what's involved?
- Researching and Developing a sustainable framework
- Keeping up

RECAP: Breaches and Records compromised

- Consider the trends across all sectors:

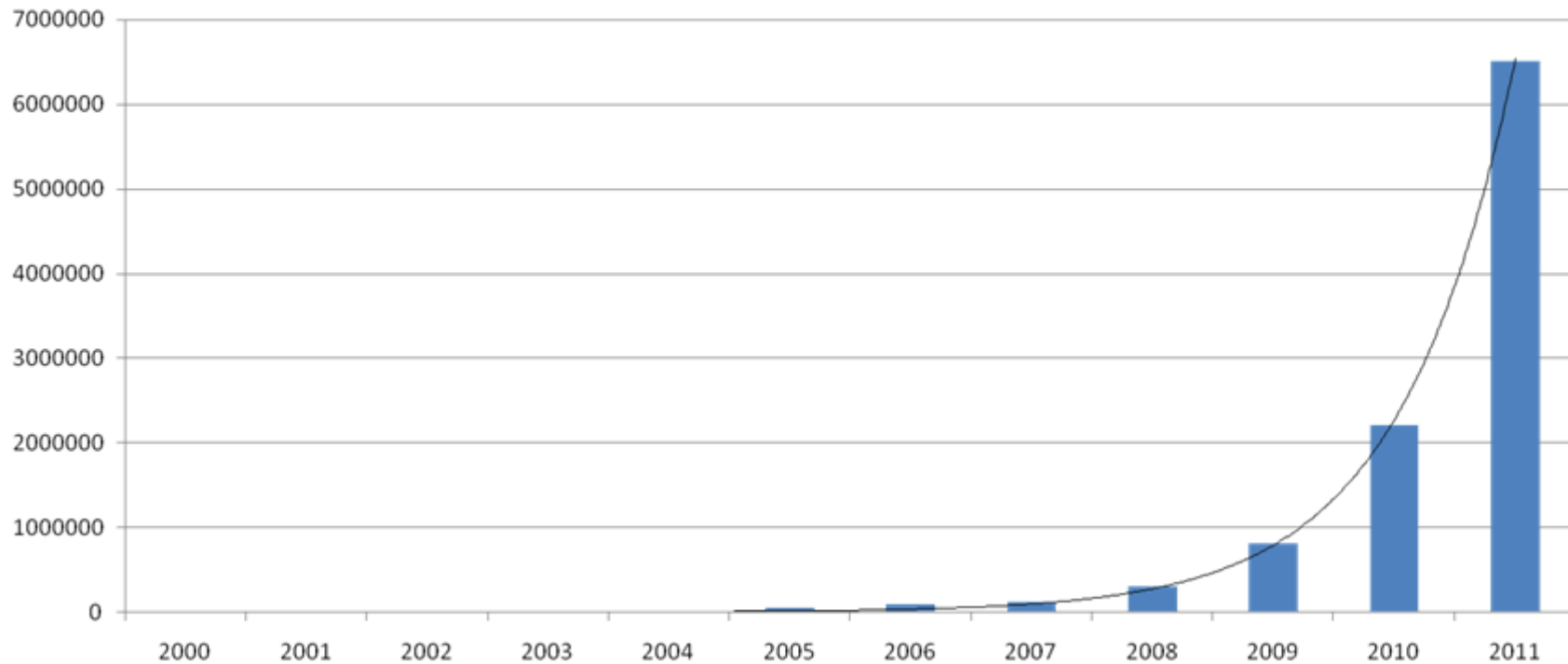


a case of – not if but when?

www.infosecurityanalysis.com

When will it stop?

Forward projection to 6.5 Billion records compromised



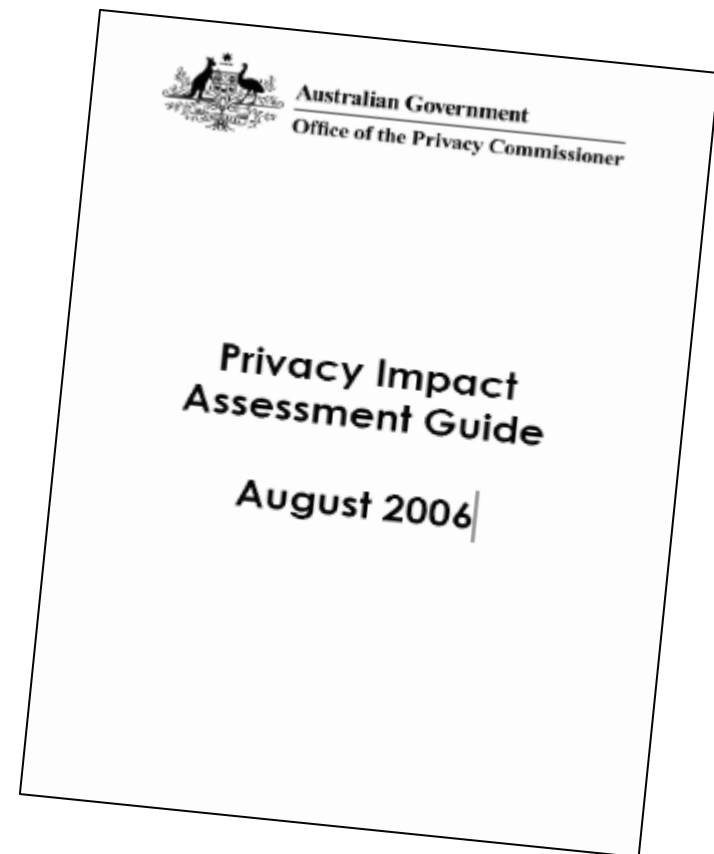
When we get serious and stop thinking it won't happen to us!

Privacy Impact Assessment (Australia)

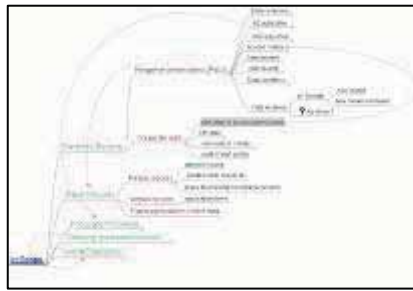
- “A PIA can be a valuable tool to help identify what needs to be done to ensure a project’s compliance with privacy legislation”

Key questions to be answered through analysis phase of the PIA:

Q#1 “Does the project comply with privacy legislation and agency-specific legislative requirements?”



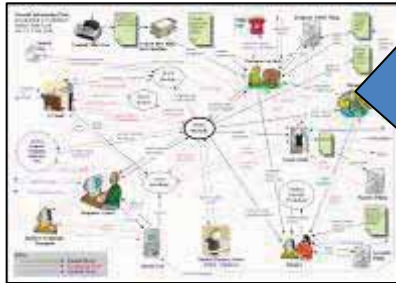
Undertaking a Privacy Impact Analysis



Scoping



Document Mapping



Mapping Information Flows

Risk	Likelihood	Impact	Risk Level	Mitigation Strategy
Loss of sensitive data due to system downtime	High	Major	High	Implement backup and recovery procedures
Unauthorized access to sensitive data	Medium	Major	High	Implement access controls and encryption
Loss of sensitive data due to hardware failure	Medium	Major	High	Implement disaster recovery plan
Loss of sensitive data due to human error	Low	Major	High	Implement user training and awareness
Loss of sensitive data due to software bugs	Medium	Major	High	Implement testing and quality assurance
Loss of sensitive data due to network attacks	Medium	Major	High	Implement network security measures
Loss of sensitive data due to insider threats	Medium	Major	High	Implement insider threat detection and response
Loss of sensitive data due to social engineering	Medium	Major	High	Implement social engineering awareness training
Loss of sensitive data due to phishing	Medium	Major	High	Implement phishing awareness training
Loss of sensitive data due to malware	Medium	Major	High	Implement malware detection and removal
Loss of sensitive data due to ransomware	Medium	Major	High	Implement ransomware awareness training and recovery plan
Loss of sensitive data due to data breaches	Medium	Major	High	Implement data breach response plan
Loss of sensitive data due to data loss prevention	Medium	Major	High	Implement data loss prevention software
Loss of sensitive data due to data retention	Medium	Major	High	Implement data retention policy
Loss of sensitive data due to data archiving	Medium	Major	High	Implement data archiving strategy
Loss of sensitive data due to data migration	Medium	Major	High	Implement data migration strategy
Loss of sensitive data due to data backup	Medium	Major	High	Implement data backup strategy
Loss of sensitive data due to data recovery	Medium	Major	High	Implement data recovery strategy
Loss of sensitive data due to data restoration	Medium	Major	High	Implement data restoration strategy
Loss of sensitive data due to data replication	Medium	Major	High	Implement data replication strategy
Loss of sensitive data due to data synchronization	Medium	Major	High	Implement data synchronization strategy
Loss of sensitive data due to data consistency	Medium	Major	High	Implement data consistency strategy
Loss of sensitive data due to data integrity	Medium	Major	High	Implement data integrity strategy
Loss of sensitive data due to data availability	Medium	Major	High	Implement data availability strategy
Loss of sensitive data due to data reliability	Medium	Major	High	Implement data reliability strategy
Loss of sensitive data due to data security	Medium	Major	High	Implement data security strategy
Loss of sensitive data due to data privacy	Medium	Major	High	Implement data privacy strategy
Loss of sensitive data due to data protection	Medium	Major	High	Implement data protection strategy
Loss of sensitive data due to data governance	Medium	Major	High	Implement data governance strategy
Loss of sensitive data due to data management	Medium	Major	High	Implement data management strategy
Loss of sensitive data due to data optimization	Medium	Major	High	Implement data optimization strategy
Loss of sensitive data due to data performance	Medium	Major	High	Implement data performance strategy
Loss of sensitive data due to data scalability	Medium	Major	High	Implement data scalability strategy
Loss of sensitive data due to data flexibility	Medium	Major	High	Implement data flexibility strategy
Loss of sensitive data due to data interoperability	Medium	Major	High	Implement data interoperability strategy
Loss of sensitive data due to data portability	Medium	Major	High	Implement data portability strategy
Loss of sensitive data due to data transferability	Medium	Major	High	Implement data transferability strategy
Loss of sensitive data due to data reusability	Medium	Major	High	Implement data reusability strategy
Loss of sensitive data due to data accessibility	Medium	Major	High	Implement data accessibility strategy
Loss of sensitive data due to data discoverability	Medium	Major	High	Implement data discoverability strategy
Loss of sensitive data due to data searchability	Medium	Major	High	Implement data searchability strategy
Loss of sensitive data due to data filterability	Medium	Major	High	Implement data filterability strategy
Loss of sensitive data due to data sortability	Medium	Major	High	Implement data sortability strategy
Loss of sensitive data due to data aggregability	Medium	Major	High	Implement data aggregability strategy
Loss of sensitive data due to data analyzability	Medium	Major	High	Implement data analyzability strategy
Loss of sensitive data due to data visualizability	Medium	Major	High	Implement data visualizability strategy
Loss of sensitive data due to data presentability	Medium	Major	High	Implement data presentability strategy
Loss of sensitive data due to data printability	Medium	Major	High	Implement data printability strategy
Loss of sensitive data due to data exportability	Medium	Major	High	Implement data exportability strategy
Loss of sensitive data due to data importability	Medium	Major	High	Implement data importability strategy
Loss of sensitive data due to data interoperability	Medium	Major	High	Implement data interoperability strategy
Loss of sensitive data due to data portability	Medium	Major	High	Implement data portability strategy
Loss of sensitive data due to data transferability	Medium	Major	High	Implement data transferability strategy
Loss of sensitive data due to data reusability	Medium	Major	High	Implement data reusability strategy
Loss of sensitive data due to data accessibility	Medium	Major	High	Implement data accessibility strategy
Loss of sensitive data due to data discoverability	Medium	Major	High	Implement data discoverability strategy
Loss of sensitive data due to data searchability	Medium	Major	High	Implement data searchability strategy
Loss of sensitive data due to data filterability	Medium	Major	High	Implement data filterability strategy
Loss of sensitive data due to data sortability	Medium	Major	High	Implement data sortability strategy
Loss of sensitive data due to data aggregability	Medium	Major	High	Implement data aggregability strategy
Loss of sensitive data due to data analyzability	Medium	Major	High	Implement data analyzability strategy
Loss of sensitive data due to data visualizability	Medium	Major	High	Implement data visualizability strategy
Loss of sensitive data due to data presentability	Medium	Major	High	Implement data presentability strategy
Loss of sensitive data due to data printability	Medium	Major	High	Implement data printability strategy
Loss of sensitive data due to data exportability	Medium	Major	High	Implement data exportability strategy
Loss of sensitive data due to data importability	Medium	Major	High	Implement data importability strategy

Recommendations

Likelihood	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost-Certain (5)
Catastrophic (5)	5	10	15	20	25
Major (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Minor (2)	2	4	6	8	10
Insignificant (1)	1	2	3	4	5

Risk	Required Actions
High Risk	Significant Risk—Immediate treatment required, i.e. should be addressed as soon as practicable.
Medium Risk	Moderate Risk—Treatment required as medium priority, i.e. should be addressed within the next few months.
Low Risk	Accepted Risk—Monitor by specific monitoring or response procedures, i.e. policies and procedures should be in place within a year.
Negligible Risk	Rejected Risk—Monitor by routine internal procedures, i.e. no special action is required.

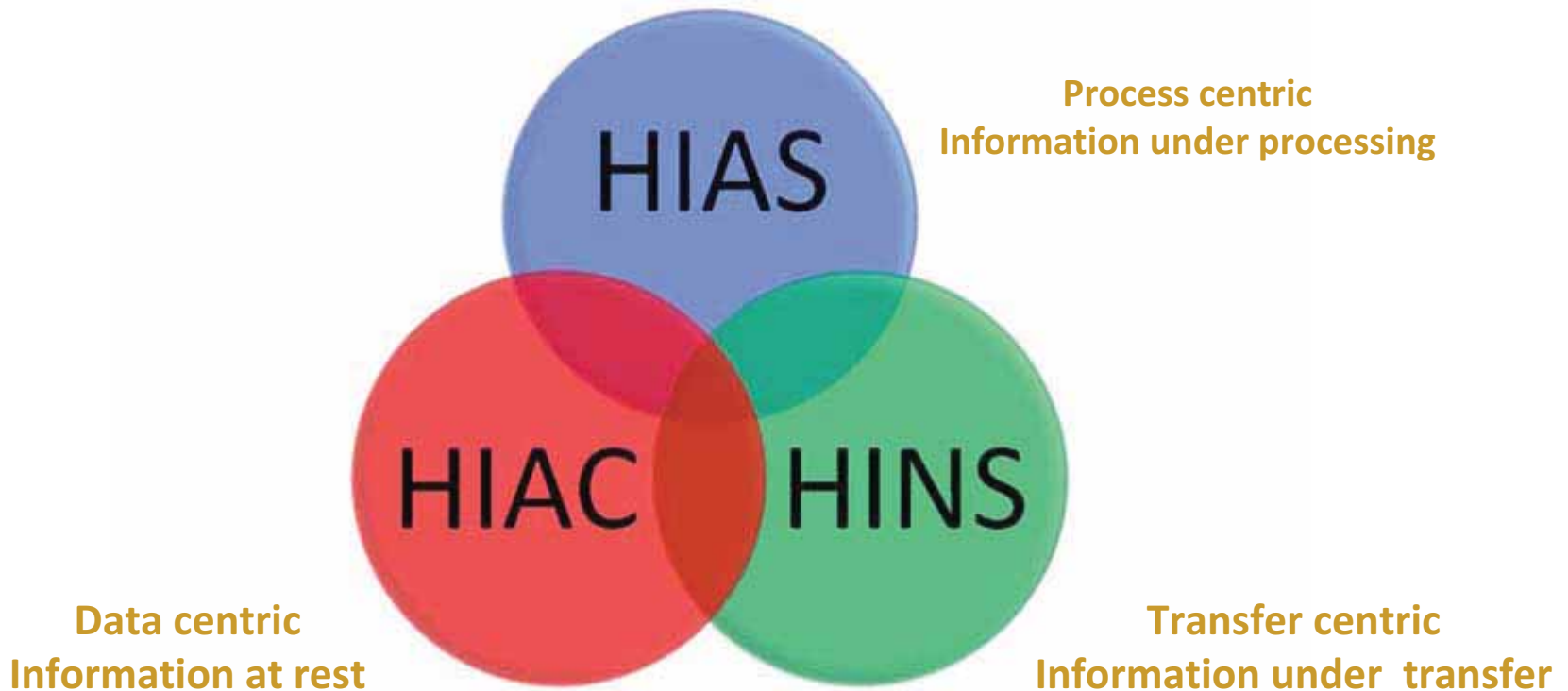
Legal Compliance Check

Article	Health Privacy Legislation	Health Privacy Legislation	Regulation
12(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 12(1)
13(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 13(1)
14(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 14(1)
15(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 15(1)
16(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 16(1)
17(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 17(1)
18(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 18(1)
19(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 19(1)
20(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 20(1)
21(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 21(1)
22(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 22(1)
23(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 23(1)
24(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 24(1)
25(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 25(1)
26(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 26(1)
27(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 27(1)
28(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 28(1)
29(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 29(1)
30(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 30(1)
31(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 31(1)
32(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 32(1)
33(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 33(1)
34(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 34(1)
35(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 35(1)
36(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 36(1)
37(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 37(1)
38(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 38(1)
39(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 39(1)
40(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 40(1)
41(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 41(1)
42(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 42(1)
43(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 43(1)
44(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 44(1)
45(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 45(1)
46(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 46(1)
47(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 47(1)
48(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 48(1)
49(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 49(1)
50(1)	Health Privacy Act 2002 (HPIA)	Health Privacy Act 2002 (HPIA)	Regulation 50(1)

Risk Analysis



Open and Trusted Health Information Systems (OTHIS)



Health Informatics Access Control (HIAC)
Health Informatics Application Security (HIAS)
Health Informatics Network Security (HINS)

End Module 1

“Introduction to key privacy issues in Health”

This Health Privacy and Security Workshop consists of 5 modules. Each module consists of 1.5 to 2 hours of small group delivery and interaction, as follows:

Module 1: Introduction to key privacy issues in Health

Module 2: How to undertake a Privacy Impact Assessment

Module 3: Risk minimisation with Health IT

Module 4: Tackling the myths of Information Security

Module 5: Managing a safe Health IT compliance framework

**THANK
YOU**