



From Mathematics to Management

Privacy and Security Risks with Electronic Health Data Integration

Peter Croll

Fellow, CSIRO's National Research Flagship
on Preventative Health

&

Professor of Software Engineering, QUT, Brisbane

ACHSE (QLD) Annual State Conference
19-20 May 2006, Gold Coast

Abstract



- This non-technical talk will look at the findings of the various risks that data integration presents to today's health managers
- then, the value of adopting highly usable IT applications that help demystify some of the complexity associated with privacy
- and, furthermore, assist in the management of the essential security protection measures, will be presented

culture change
– shifting sands



- **Information Technology & Culture Change?**
 - **Safety & Quality**
 - **Remote Access and Services**
 - **High Speed Access**
 - **Efficiency Gains**
 - **Outsourcing Capabilities**
 - **Preventative Health**
 - **Satisfaction & Fulfillment**

Linked Health Data



- This all demands linking systems together (*new and existing*)

- linking data
 - linking technologies
 - linking enterprises
 - linking people

across Departmental, Organizational and State boundaries

Minimising the Privacy & Security Risks of Linked Health Data



- What are the risks?
- How can we reduce them?
- What techniques protect data for:
 - clinical care
 - health administration
 - and secondary usage in research studies?

The necessary trust can be fragile and easily broken through well publicized incidences!

“Information Technology makes extensive use of complex mathematical techniques to protect data. This includes both encryption and statistical analysis (e.g. the probability of back tracking with de-identified data or the probability of adverse incidences occurring).”

All the mathematics is pointless if the system is not well managed!

- Do health managers understand the maths?
- Should they have to?

To answer these questions



- What do you need to understand about securing linked systems?
- What **new risks** does integration and access to electronic health data bring?
- How can you do an effective risk analysis?
- Can we realistically look at **health care provision as a whole**?
- Do privacy and security guidelines / legislation help or hinder?
- What role does **Trust** play?
- How relevant is the International scene?

Security Concerns



Websites exist (<http://www.sans.org/top20/>) that are dedicated to reporting on the most current:

‘Top 20 Internet Security Vulnerabilities’

- Currently the most venerable issue under **cross-platform** services is ‘**Backup Software**’.
- This is a valuable asset for any organization and typically runs across several servers, but the trend has been towards small number or a single large server to ease the administration overheads.
- Unfortunately **much of the commercial software has exploitable vulnerabilities** allowing systems to be completely compromised.
- That is, an attacker can leverage these flaws for an enterprise-wide compromise and **obtain access to the sensitive backed-up data**.

Bureaucratic Concerns



The inability to access medical data could put valuable medical research at risk!

"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"

said Robert Souhami, a cancer researcher at University College London.

"and this is a detriment to public health."

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.

Privacy Concerns



The Australian (IT Today)
Tuesday March 21, 2006
Karen Dearne, Health correspondent

Consent Dispute in Health Project

"Mounting privacy and consent issues threaten to derail NSW Health's long awaited electronic health records pilot, due to start in the Hunter Region"
"NSW acting privacy commissioner John Dickie met NSW Health yesterday over concerns that some aspects of the trial may be in breach of the state's health record and information privacy laws."

A compromise was reached whereby the precedence was set to allow the system to be regarded as an 'opt-out' option.

Katherine McGrath, NSW Health deputy director-general for health system performance, stated "We're not trying to do this under the covers; we know lots of people are anxious about the changes, but the opt-in model was found to be too technically difficult to do, for a whole range of reasons."

Privacy and Related Legislation in Australia



Commonwealth:

- [Privacy Act 1998](#)
 - ❑ 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 b/ATO & other assistance agencies)
- [Freedom of Information Act 1982](#)
- [Archives Act 1983](#)
- [Crimes Act 1914](#), Pt VIIC (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 nor administrative privacy regime, but see [discussion paper](#) (released 20 May 2003) and note that privacy legislation is [intended](#) to be introduced, [possibly before Christmas 2005](#)
- [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 for 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)

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](#)

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 Video 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 1992](#)

Tasmania:

- [Personal Information Protection Act 2004](#)
- [Freedom of Information Act 1991](#)
- [Archives Act 1983](#)
- [Annulled Convictions Act 2003](#) (spent convictions)
- [Listening Devices Act 1991](#)
- [Telecommunications \(Interception\) Tasmania Act 1999](#)

NEHTA states that privacy protection in Australia is a complex patchwork: “It is considered possible to navigate the existing privacy environment although this is not without some risk and may require future changes”.

Safety Concerns



Thousands of children at risk after computer fault

Babies miss injections as privatised NHS monitoring system breaks down

Jo Revill, health editor
Sunday February 26, 2006

Observer

As many as 3,000 babies and toddlers may have gone without crucial vaccinations because a privatised NHS computer system has failed to monitor which children are due for jabs and whether they have received them.

An Observer investigation has found that the child health information system, introduced last summer as part of the government's £7 billion IT programme, has **derailed the country's entire vaccination programme** leaving health staff resorting to slips of paper to work out who needs immunising.

Several women whose babies were stillborn have received letters asking them to take their babies for their first vaccinations.

Offshoring Concerns



San Francisco Chronicle

DAVID LAZARUS

A tough lesson on medical privacy

Pakistani transcriber threatens UCSF over back pay

Wednesday, October 22, 2003

"Your patient records are out in the open... so you better track that person and make him pay my dues."

A woman in Pakistan doing cut-rate clerical work for UCSF Medical Center threatened to **post patients' confidential files on the Internet** unless she was paid more money. To show she was serious, the woman sent UCSF an e-mail earlier this month with actual patients' records attached.

The **violation of medical privacy** - apparently the first of its kind - highlights the danger of "**offshoring**" work that involves sensitive materials, an increasing trend among budget-conscious U.S. companies and institutions...

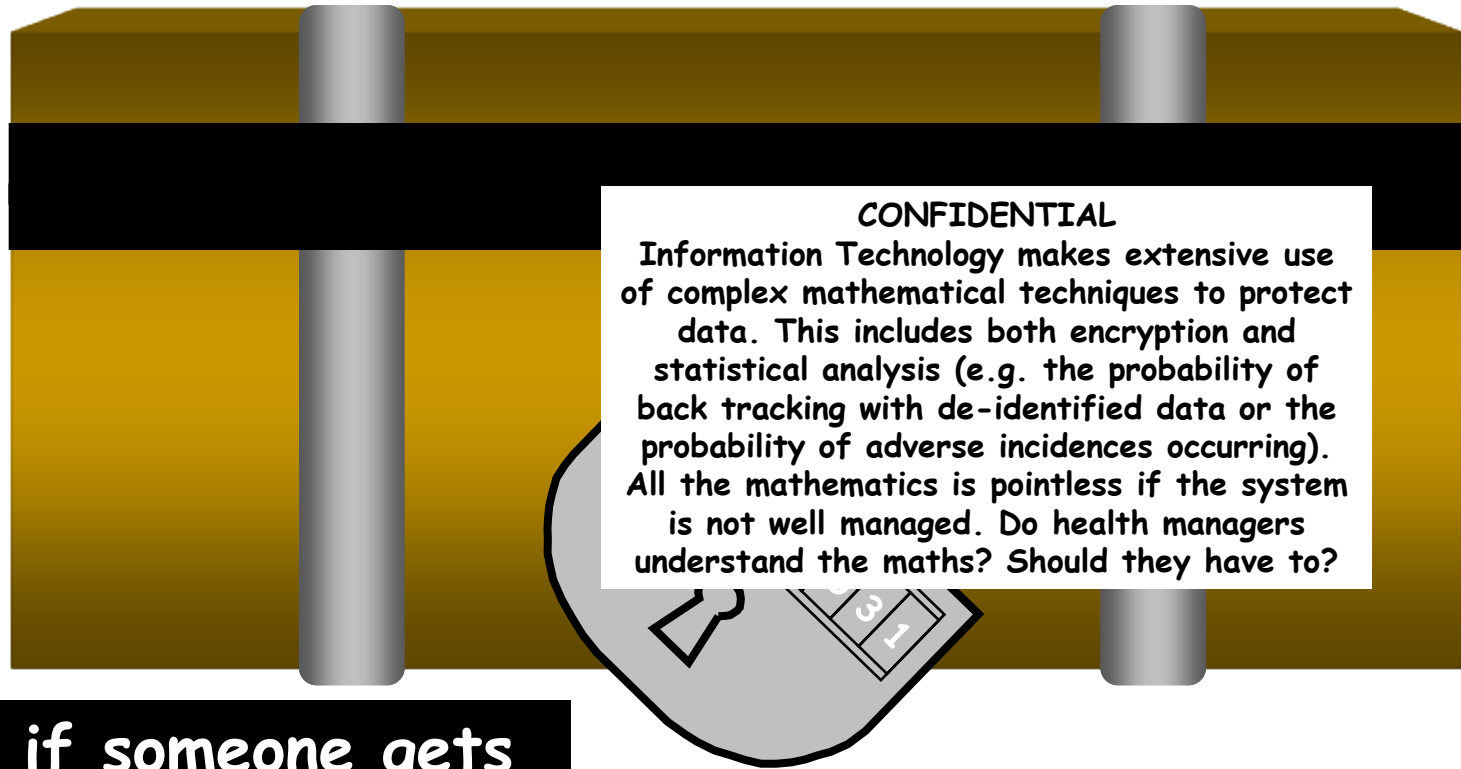


- Messages and Data can be protected through **encryption**
- This is based on an age old technique of **scrambling** information
- A **numerical key** (often generated from a password) provides the encryption (lock) and decryption (unlock)
- **Single Key Encryption** is commonly used and can be very effective
- Here is an example of how it operates....

Single Key Cryptography



$2^{128} = 34028236692093846346337460743177938721$



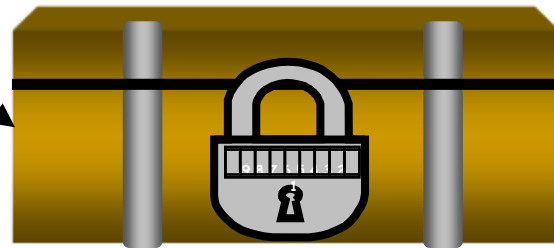
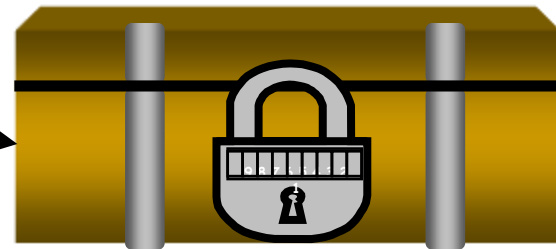
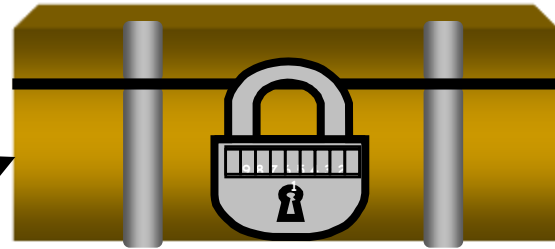
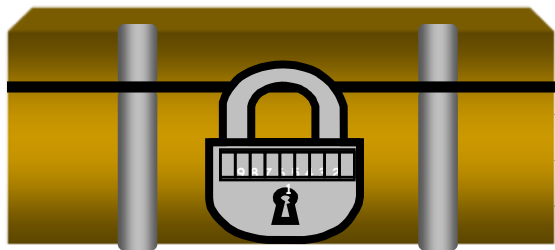
CONFIDENTIAL
Information Technology makes extensive use of complex mathematical techniques to protect data. This includes both encryption and statistical analysis (e.g. the probability of back tracking with de-identified data or the probability of adverse incidences occurring). All the mathematics is pointless if the system is not well managed. Do health managers understand the maths? Should they have to?

What if someone gets hold of your key - would you know?

Shared single key



How do we manage these keys?
What if someone's key gets compromised?



Single Key

987654321

Public / Private Keys



- It is not always convenient to have to use the phone (or a dispatch rider) to **distribute** our secret numbers
- Also, with single keys once one person has been compromised **everyone** is vulnerable
- The task of reissuing single keys **is expensive** and the original vulnerability (e.g. a virus) might still be resident on someone's system
- A **Public / Private Key** pair algorithm can be used, such as RSA to overcome these restrictions and vulnerabilities.

RSA Public Key Algorithm



1. Choose two (in practice, large 100 digit) prime numbers p and q and let $n=pq$.
2. Let P_i be the block of (plain) text to be encrypted. Actually P_i is the numerical equivalent of the text which may either be single letters or blocks of letters, just as long as $P_i < (p - 1)(q - 1) = \phi(n)$.
3. Choose a random value E (usually small) such that E is relatively prime to $\phi(n)$. Then the encrypted text is calculated from

$$C_i \equiv P_i^E \pmod{n}.$$

The pair of values (n,E) act as the public key.

4. To decode the ciphertext, we need to find an exponent D , which is known only to the person decoding the message, such that

$$DE \equiv 1 \pmod{(p - 1)(q - 1)}.$$

Note that $\phi(n) = \phi(pq) = (p - 1)(q - 1)$. Then we may calculate


$$C_i^D = (P_i^E)^D = P_i^{DE} \equiv P_i \pmod{n}.$$

This step is based on the following result:

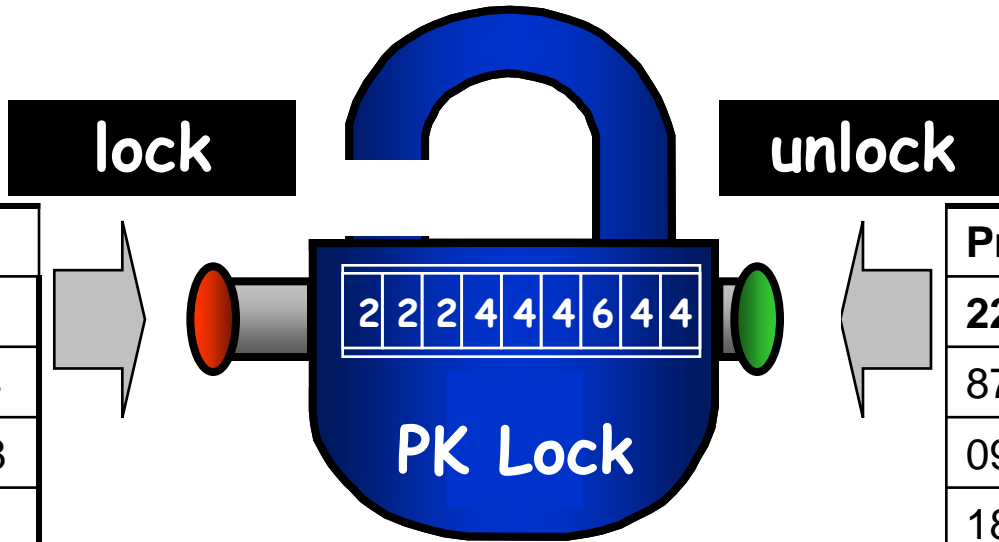
$$(a^x)^y = a^{xy} \equiv a^z \pmod{n}, \text{ where } z \equiv xy \pmod{\phi(n)}.$$

Public and Private Keys Sets



	Public		Private
Peter	2766234918872983691		7876829817094710092
Lyn	8762987654289119053		1123445466686299188
Ming	0987088780236928273		1987264398326782988
Dr D	1837677382009927340		0987698327345673821
Ben	3872961098374598206		1922748847579391100

Public Key Lock



Public (Directory)	
Peter	99981111
Lyn	11234454
Ming	26782988
Dr D	09873821
Ben	19228470

Private (Secret Password)	
222444644	(Peter)
876298765	(Lyn)
098708878	(Ming)
183767738	(Dr D)
387296109	(Ben)

Using the PK Lock



Someone has sent me a strong box locked using my public key

Only the paired private key will open it - (nobody else should know this key)

PK lock limitations



- This method **does not authenticate** who sent the message
- Anyone can find my public key and send a message **masquerading as someone else**
- This is where **Digital Certificates** are useful
- DC's allow you to encrypt a special message that could **only have been encrypted by you**
- Essentially – we put a box inside the box which has been PK locked by **reversing the keys** round
- i.e. locked using my private key – you open it using my public key – then it must have come from me!

Conclusions



- **highly application dependent and dynamic**
- **trust in e-Health fragile**
- **increase understanding of interdependencies**
- **experts' prediction significantly deviates from perceived risks**
- **modify methods to accommodate perceived risks**
- **survey consumer attitudes**
- **international**
- **develop technology to support compliance with policy and security policy generation**