AUSTRALIAN COMPUTER SOCIETY

an Education Across the Nation (EdXN) presentation

Privacy is your Problem

- how to become empowered, not enslaved

learn the critical risks and how you can protect personal information

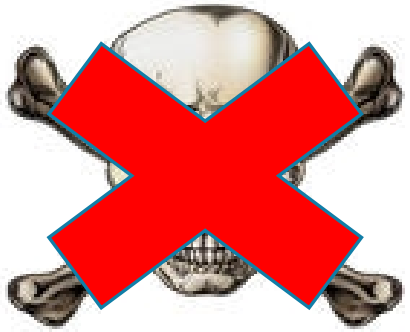
DR PETER R. CROLL

PRC@PETERCROLL.COM

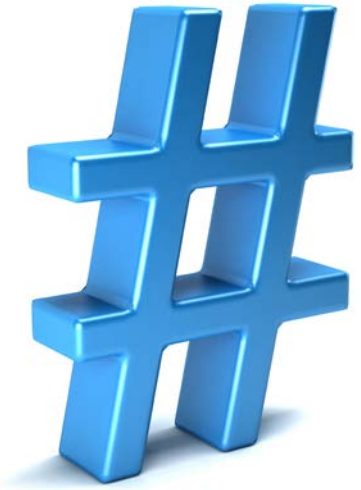
to prevent any confusion

a bit about me

- 30 years+ experience in IT - I've always worked in risk / risk minimization
- Firstly in machine and aircraft control systems - last 15 years focus on Health IT
- Chair of Australian and the International workgroups on Health Privacy and Security
- Australian Law Reform technical committee, Standards committee IT14
- Many submissions to government changes to legislation and policy
- Now work as a Cyber Security and Privacy consultant –industry, gov. and professional societies
- I publish ‘How-To’ eBooks to assist practitioners, particularly SMEs



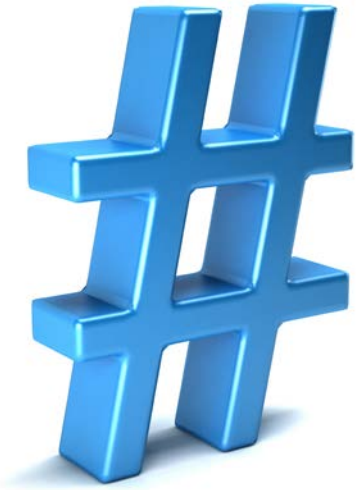
topics



- **is privacy dead?**
- **privacy law changes**
- **holistic view of privacy**
- **calculating privacy risks**
- **privacy analysis – case study**
- **privacy-by-design**
- **‘My Health Record’**
- **social networking**
- **the way forward?**

topics

- **is privacy dead?**
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- social networking
- the way forward?



is privacy dead?

“You have zero privacy anyway. Get over it.”

Scott McNealy (Co-founder, Sun Microsystems) 1999

is privacy dead?

“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place”

Eric Schmidt (CEO, Google) 2009

is privacy dead?

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”

Edward Snowden, 2015

is privacy dead?

“We believe that people have a fundamental right to privacy. The American people demand it, the constitution demands it, morality demands it”

Tim Cook (CEO, Apple) 2015

is privacy dead?

“Digital surveillance is worse than anything George Orwell could have foreseen”

Joseph Cannataci (UN Privacy Chief) 2015

SMH thinks Privacy is dead!

“On 13 Oct this country's entire communications industry will be turned into a surveillance and monitoring arm of at least 21 agencies of executive government”

“The electronically logged data of mobile, landline voice (including missed and failed) calls and text messages, all Aus emails, download volumes and location information”

“Mandatorily retained by Australian telcos and ISPs or face a $2 Million fine”

Australian Government
Office of the Australian Information Commissioner

Ben Grubb and Telstra Corporation Limited
[2015] AICmr 35 (1 May 2015)

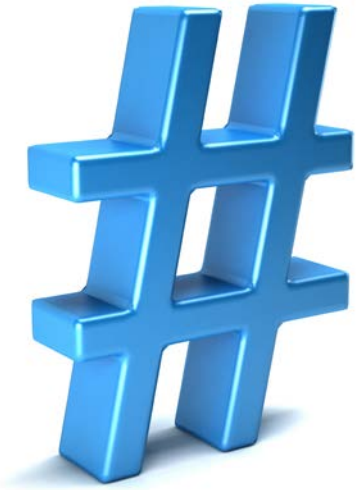
Determination and reasons for determination of Privacy Commissioner, Timothy Pilgrim

Complainant:	**Ben Grubb**
Respondent:	**Telstra Corporation Limited**
Determination date:	**1 May 2015**
Application number:	**CP13/01119**
Catchwords:	**Privacy — Privacy Act — National Privacy Principles — (CTH) *Privacy Act 1988* — s 52 — NPP6.1 — Access**

Ashley Madison or 'jihadi' content sites, may in effect be discoverable without the need for a warrant.”

topics

- is privacy dead?
- **privacy law changes**
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- social networking
- the way forward?



new laws

- Privacy Act - Updated 12 March 2014 - after major review

  Now contains 13 new Australian Privacy Principles (APPs)

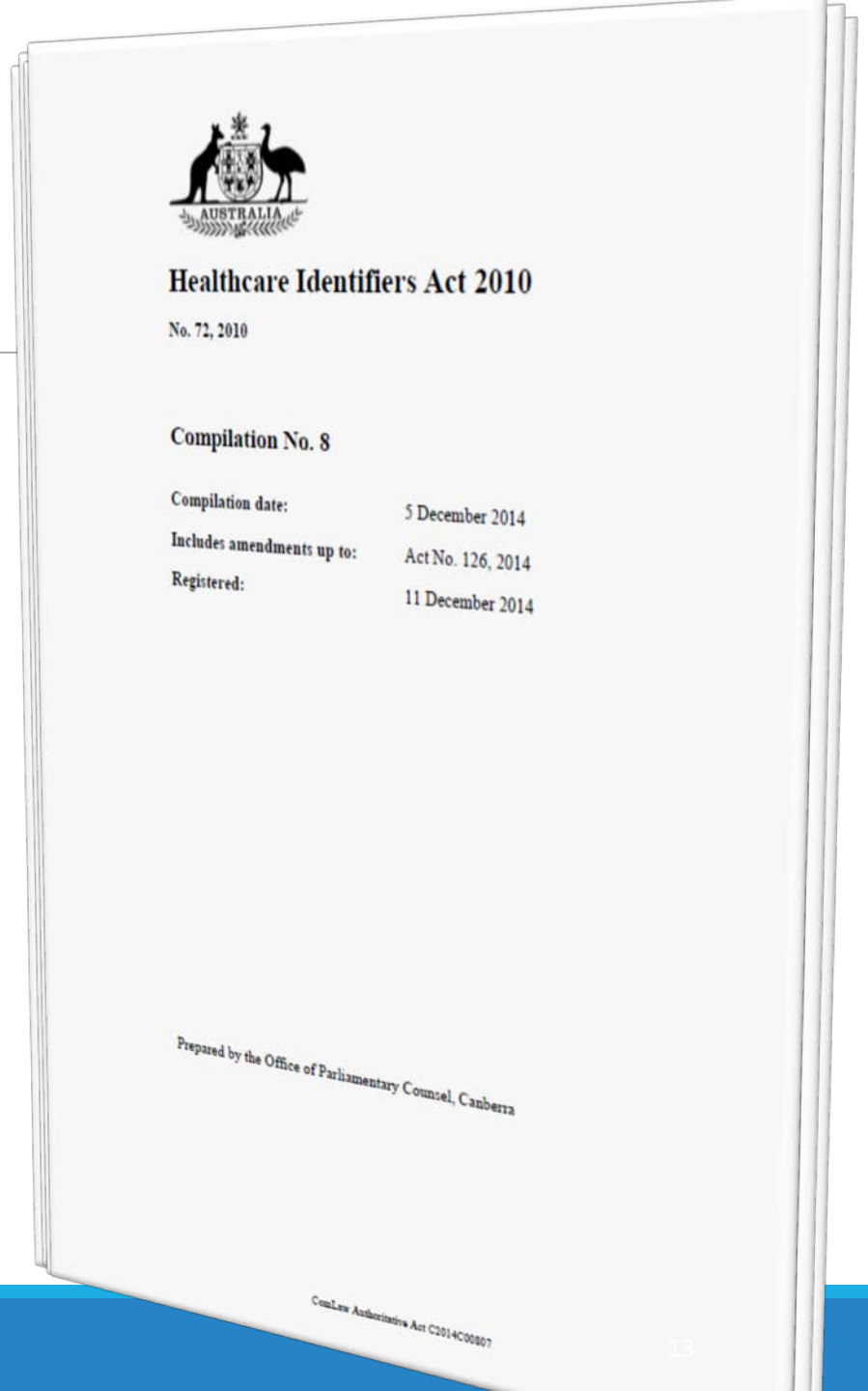
- Telecommunications (Interception and Access) Amendment (Data Retention) - Act 2015

- Personally Controlled Electronic Health Act

  Centralised government health record for all Australians

- Health Identifiers Act

  Every Australian assigned a unique 16 digit ID


AUSTRALIA

Healthcare Identifiers Act 2010

No. 72, 2010

Compilation No. 8

Compilation date: 5 December 2014

Includes amendments up to: Act No. 126, 2014

Registered: 11 December 2014

Prepared by the Office of Parliamentary Counsel, Canberra

ComLaw Authoritative Act C2014C00807

Privacy law changes – Australian Privacy Principles

APP 1 – open and transparent management of personal information

- more prescriptive requirements for privacy policies

APP 2 – anonymity and pseudonymity

- Provide individuals ,where practical, with the option of dealing with entities anonymously (e.g. pseudonym)

APP 3 – collection of solicited personal information

- Collect from Individual and only collect 'Sensitive' with consent

APP 7 – direct marketing

- When individual consents or would expect this and if they can opt-out easily

13 APPs now (previously 10 NPPs or 11 IPPs)

APP 8 – cross-border disclosures

- Agency must take reasonable steps to ensure overseas recipients comply with APPs

APP 11 – security of personal information

- Steps to destroy/de-identified when no longer needed

APP 12 – access to personal information

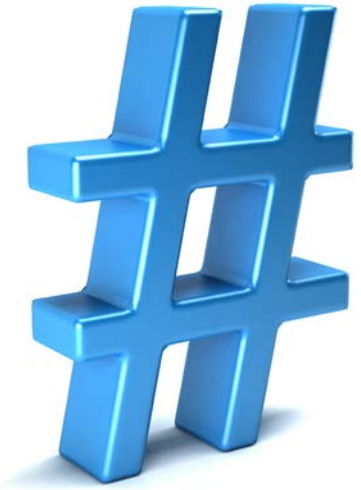
- Process for individuals to access and correct their personal information

APP 13 – correction of personal information

- Correct so that its up-to-date, complete, relevant, accurate and not misleading

topics

- is privacy dead?
- privacy law changes
- **holistic view of privacy**
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- social networking
- the way forward?



holistic view of privacy

Good **SECURITY** is essential but far from the whole story

PRIVACY protection goes much further - it requires a holistic view

What if **SECURITY** is breached but the information disclosed can not identifying you?

What if personal information is disclosed by other means? - e.g. an overseas organizations hassling you to buy the latest insulin pumps since they were informed that you are a diabetic.

What if authorized users look up your personal information when they have no moral right to do so? - e.g. your sensitive information is not part of their case load?

That is, they were authorized by the system since they work at the organization concerned. They might be your relatives or acquaintances!

Your **PRIVACY** is breached (although the **SECURITY** may not have been)

confidentiality and trust

CONFIDENTIALITY is about not disclosing secret information

Patient **CONFIDENTIALITY** is about the healthcare practitioners keeping personal sensitive health information ‘secret’ from anyone who doesn't ‘need-to-know’

In business, ‘commercial in confidence’ relates to **CONFIDENTIALITY** of company secrets

TRUST is the confidence you place in others to keep secrets and protect you

What if you provide your contact list to an organization (or an app) and they later use this in ways you would never had agreed to when you originally provided it?

They may use your contact list to sell services and claim it was from your recommendation

A breach of organizational **TRUST**

safety

What if the personal (possibly sensitive) information that is breached causes you or an acquaintance harm?

SAFETY is about taking measures to minimize harm

What if a **SECURITY** breach causes important information to be:

- corrupted (poor integrity) or
- really slows the system down (poor availability) or
- makes it impossible to retrieve (inaccessible)?

This might cause harm to either ‘you’ or the ‘system’ – which in turn may cause harm to the business.

harm

HARM to be concerned about with regard to IT systems:

Harm to:

- the individual (embarrassment, loss of finance, social status, job or respect);
- the system (integrity, availability or accessibility);
- the business (trust, financial);
- the community and environment (confidence, respect, financial and damage).

risks

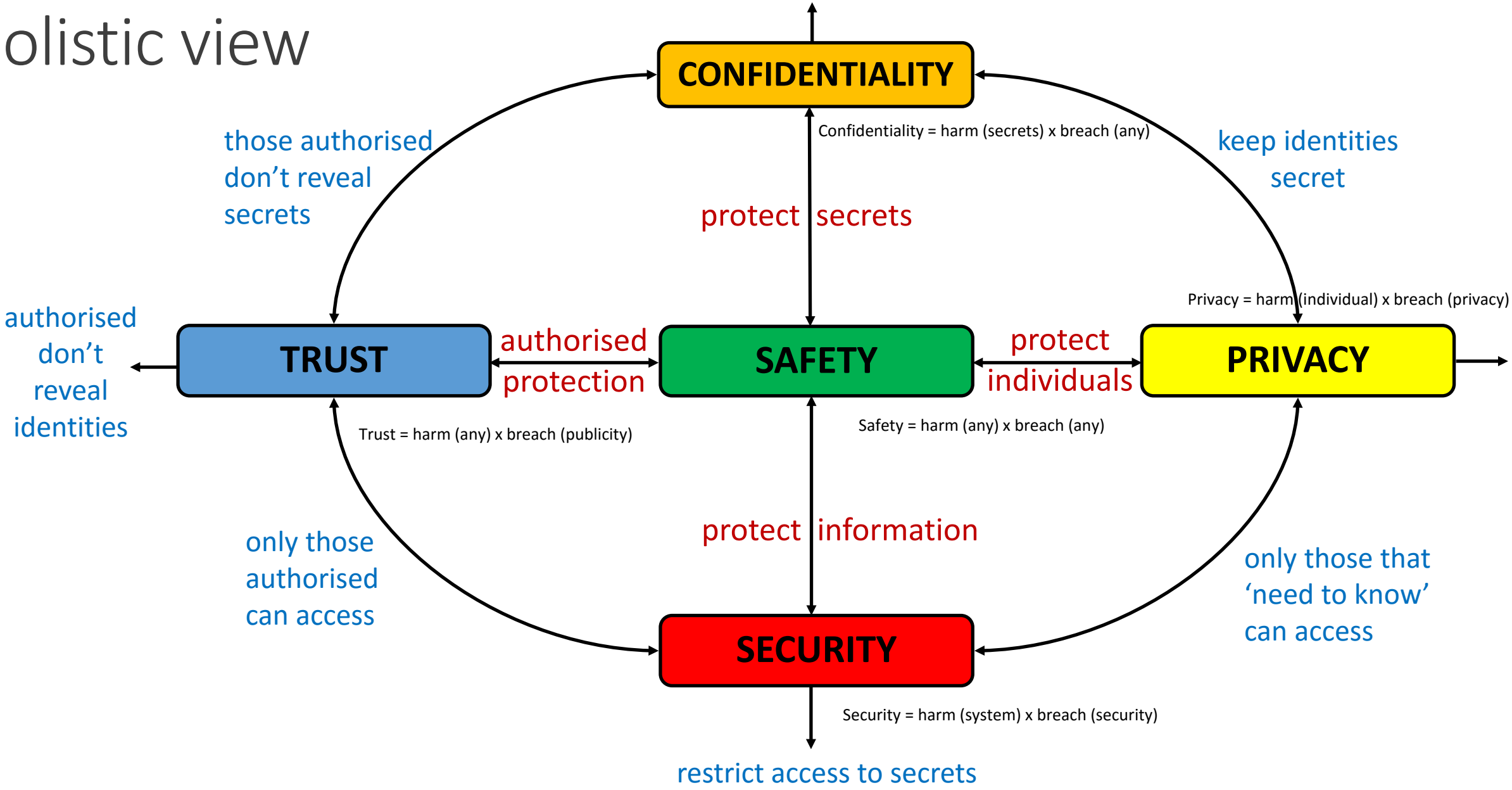
Minimising the IT RISKS of:

- unauthorised access (**SECURITY**)
- inappropriate disclosure regarding identifiable individuals (**PRIVACY**)
- inappropriate disclosure of secret/protected information (**CONFIDENTIALITY**)
- unexpected organisational behaviour (**TRUST**)
- harm to individual, system or secrets (**SAFETY**)

"exposure to the chance of injury or loss;
a hazard or dangerous chance"

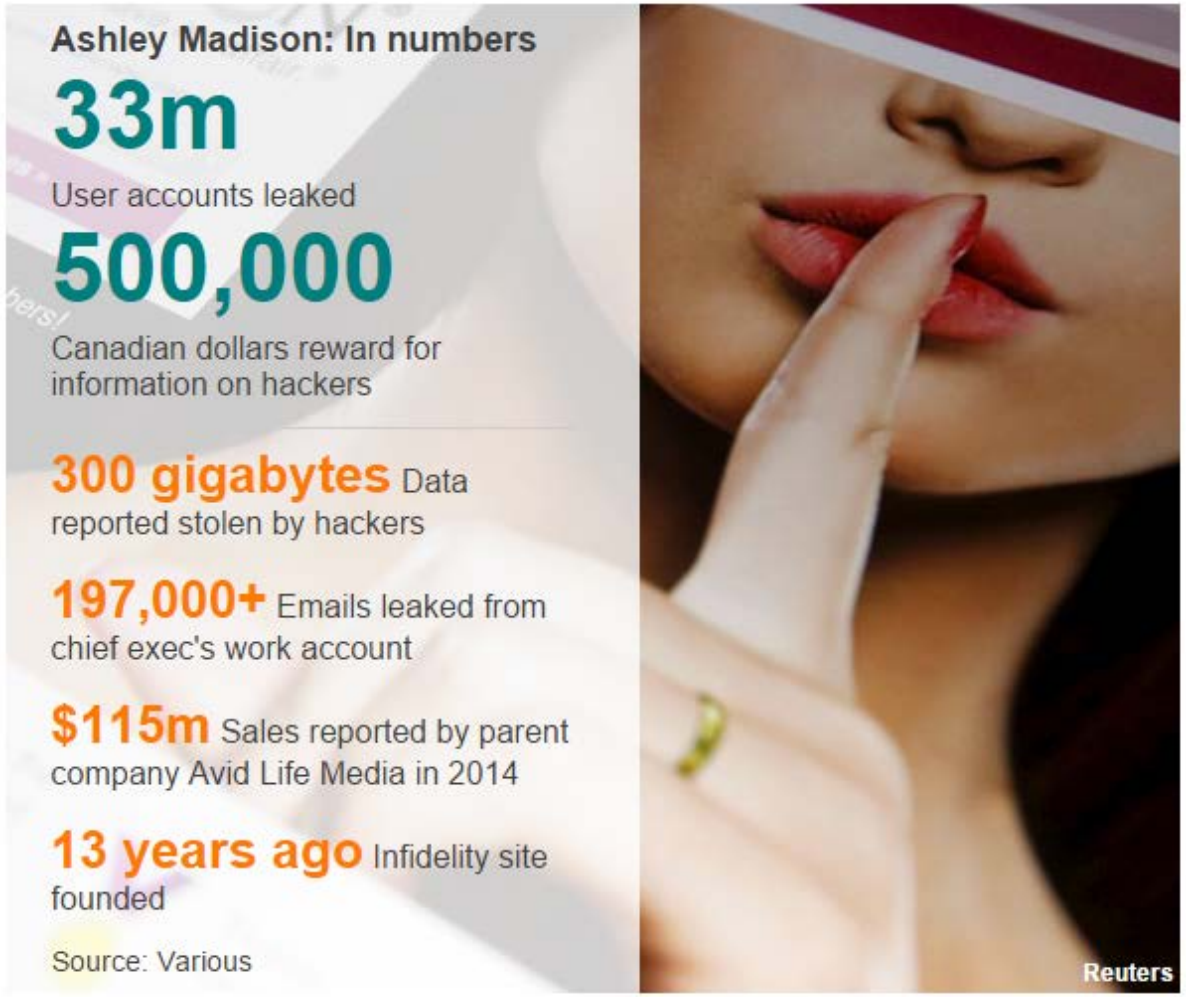
['Risk' definition: Macquarie Dictionary]

holistic view



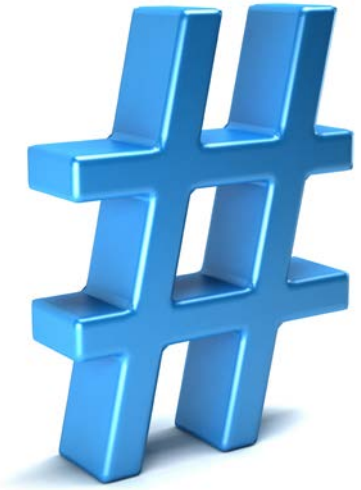
recent example

- **breach (security)** from disclosure of 33 million accounts to unauthorised hackers
- **breach (publicity)** occurred when criminals threatened to expose accounts on the Internet
- **breach (privacy)** resulted when personal data was published for all to download
- 'significant' **harm (individual)** and **harm (business)** as a consequence
- **SECURITY** and **PRIVACY** risks may have now been minimised by the company
- **TRUST**, **CONFIDENTIALITY** and **SAFETY** risk levels remain 'Very High'



topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- **calculating privacy risks**
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- social networking
- the way forward?



calculating privacy risks

To calculate privacy risk levels:

You need to know the chance of a breach occurring

this can be measured in likelihood (i.e. frequency) of a breach occurrence per annum

You also need to know the impact (consequences) once a breach has occurred

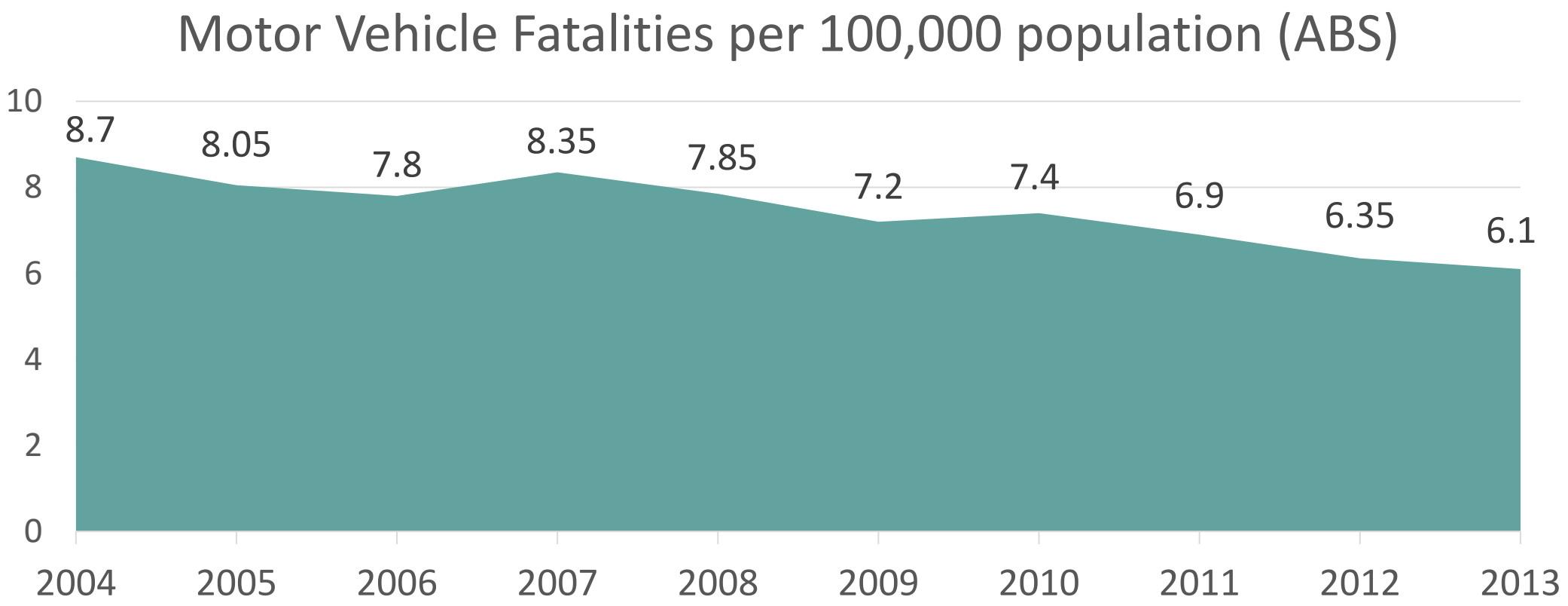
this can be measured in 'number of records' or 'cost to business', etc.

These factors are much easier to estimate when you have a reliable history of occurrences and you are dealing with well understood technologies, e.g.:

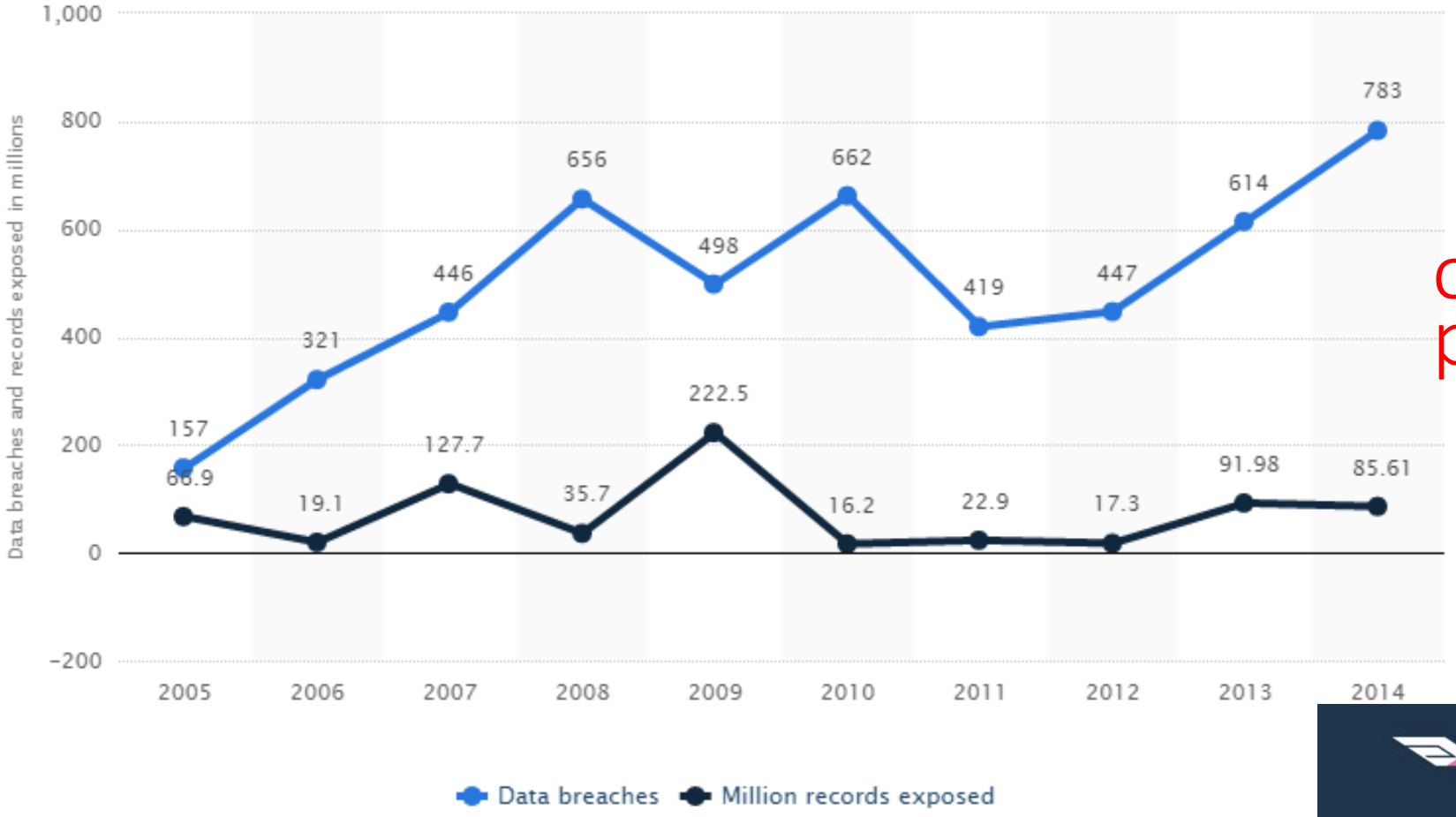
EASIER – risks from Australian postal services misdelivering personal letters

HARDER – risks from new mobile APP to access your personal details from a company database

example risk history



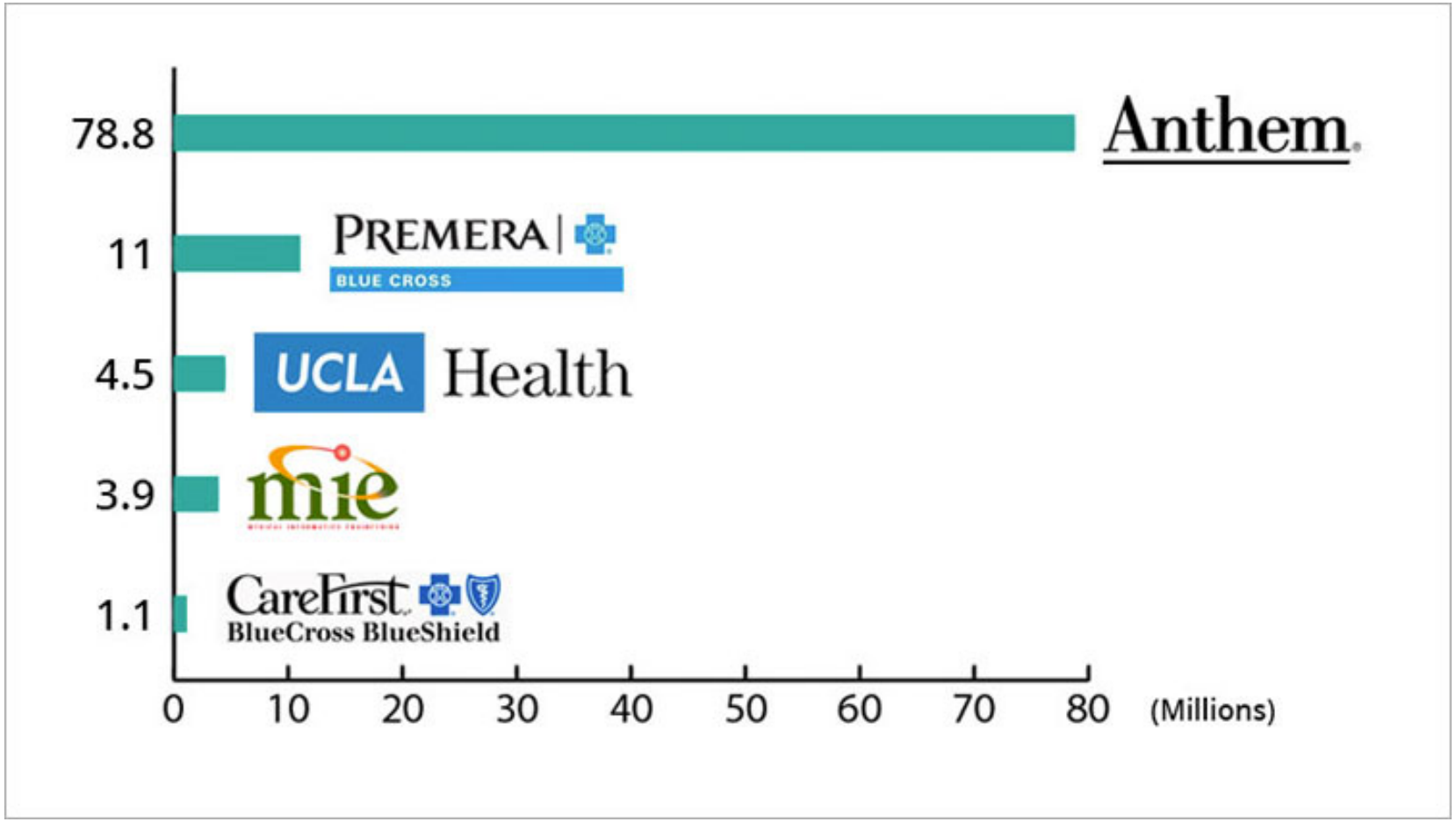
Annual number of data breaches and exposed records in the United States 2005-2014



offers some predictability?

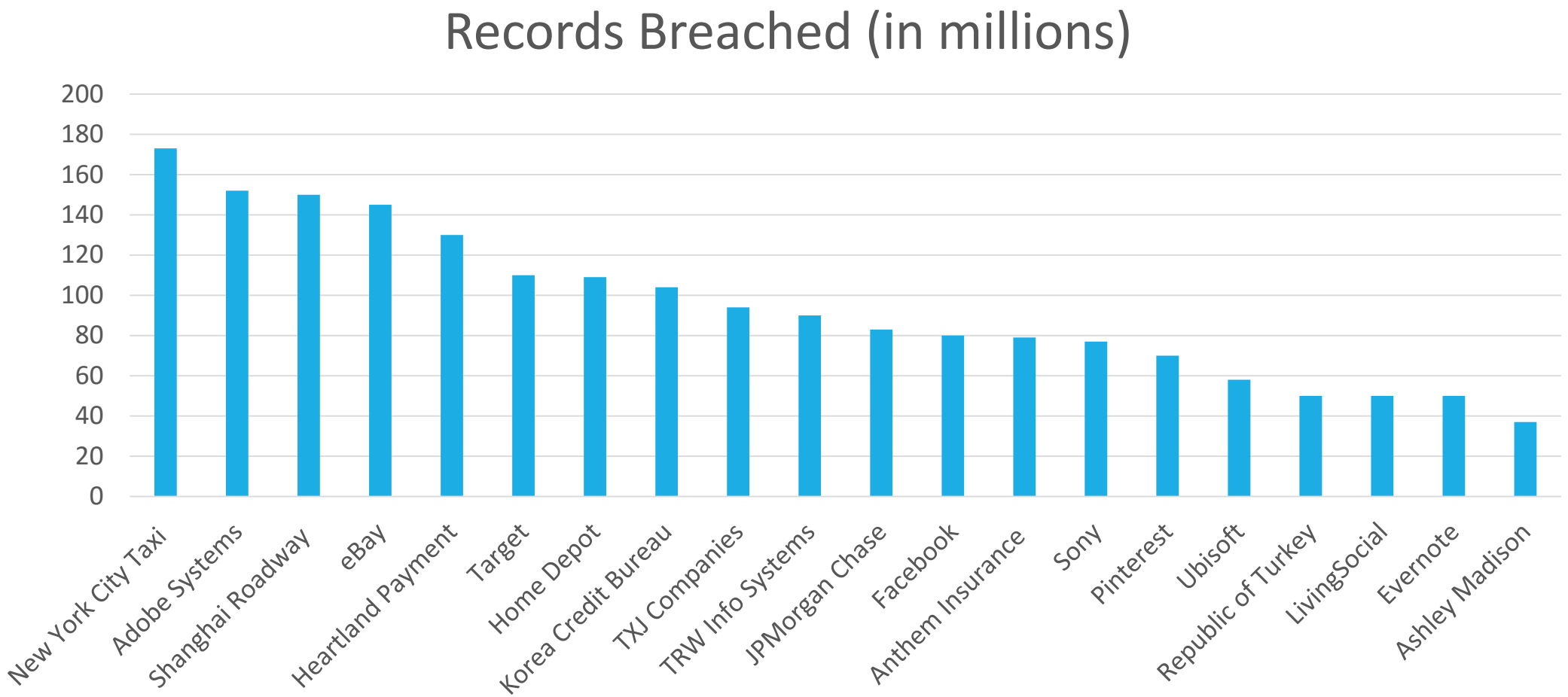
DIGITAL GUARDIAN
Formerly VERDASYS

Over 100 Million Affected in 2015 Healthcare Data Breaches

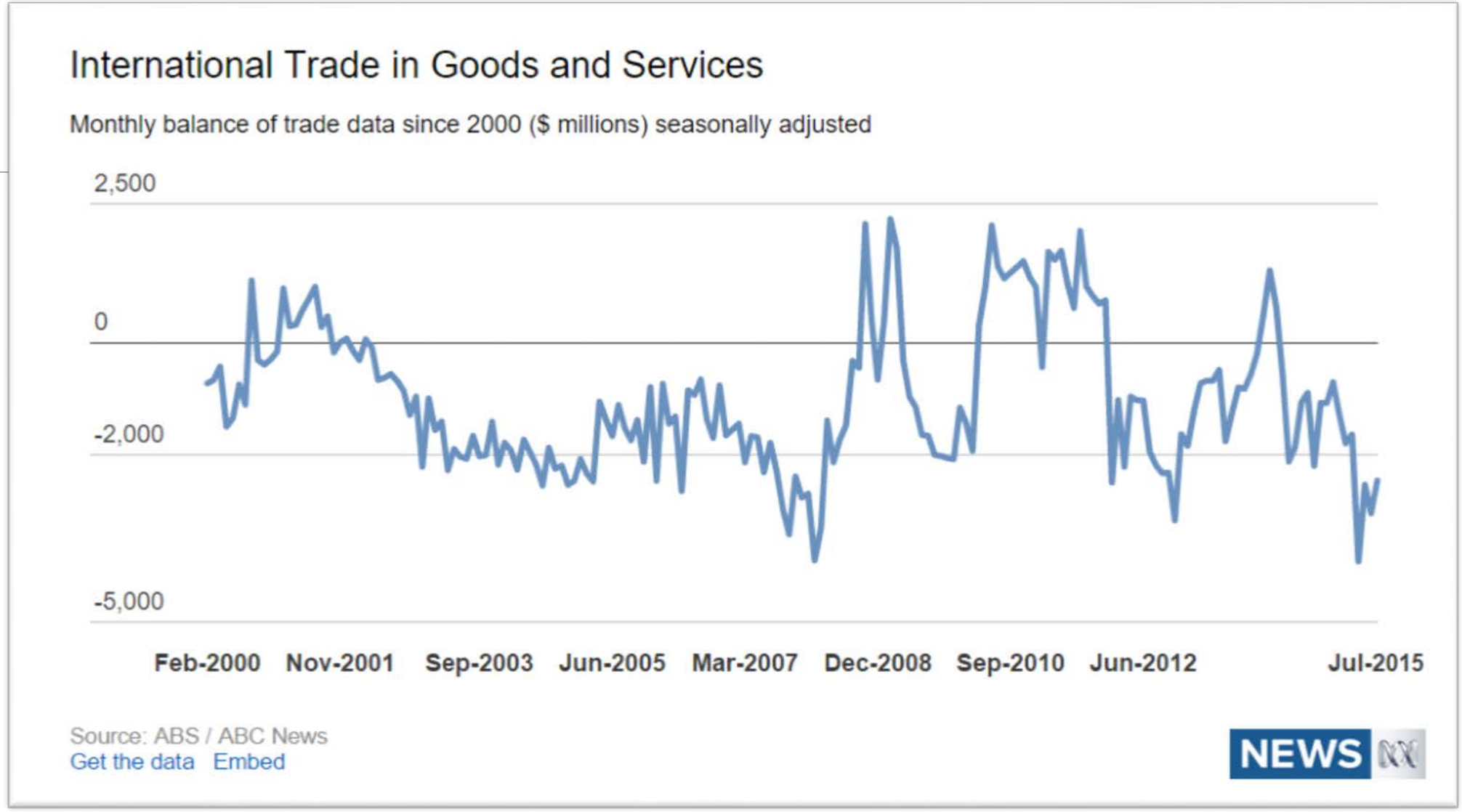


Largest Reported Data Breaches

BUSINESS INSIDER AUSTRALIA

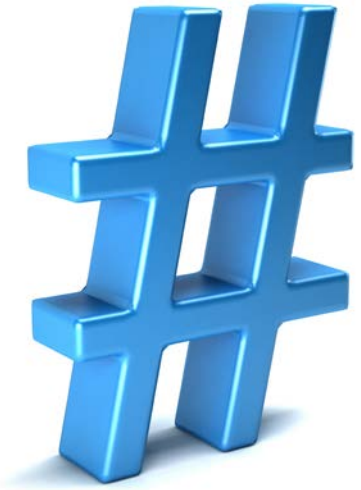


consider highly volatile?



topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- **privacy analysis – case study**
- privacy-by-design
- ‘My Health Record’
- social networking
- the way forward?



privacy analysis - case study

Privacy Impact Assessment (PIA)

"Online Information Management for Members"

YourOnlineFriends.com is an Internet-based service to assist parents or guardians of children with special medical needs.

They plan on extending their services to allow online applications for new members and information updates by existing members.

This will include entry of personal information, some of which is highly sensitive.

This PIA considers the impact on privacy through the addition of these new services.

areas of concern

The main concerns:

- lack of system documentation from third party IT service providers
- use of shared resources (e.g. USB drive, Dropbox, shared network drives, etc.)
- a necessity to strengthen network security measures

Other concerns:

- unnecessary collection of some personal information
- not providing an opt-out from direct marketing
- the focus on information security rather than privacy at the annual audits

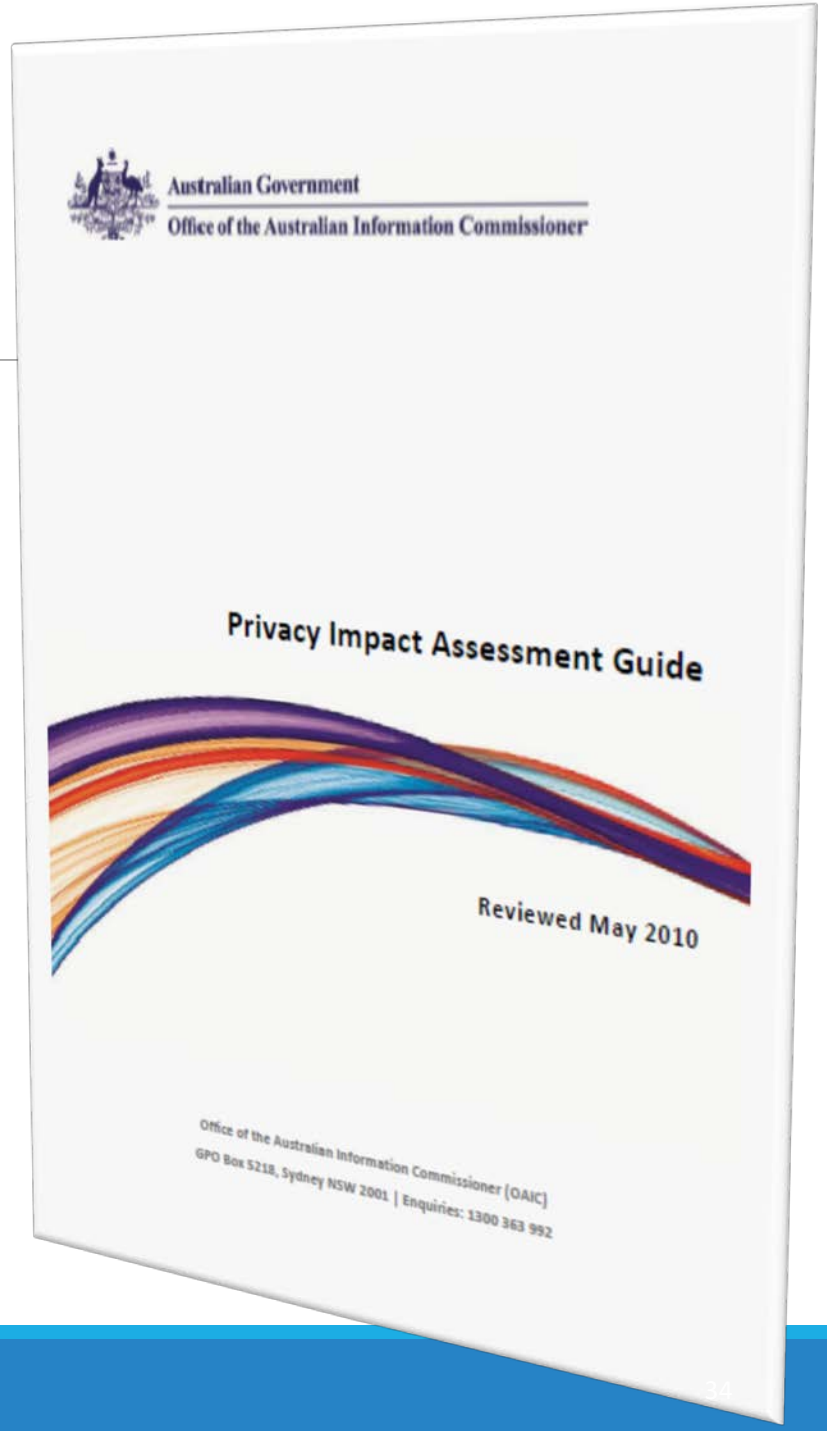
areas of concern (2)

Recommendations:

- some practices by staff members resulting in unintentionally violation of the Australian Privacy Principles
- introduction of staff privacy training
- **YourOnlineFriends.com** makes use of third party service providers yet it is still responsible for the privacy of its customers
- the inclusion of privacy compliance in third-party service agreements
- maintaining ongoing compliance and the publication of an abridged PIA

PIA

- The Australian government recommends undertaking a PIA
- This case study identified twenty potential privacy impacts.
- Privacy impact was estimated ranging from High-level to Medium to Low-level risks.
- Report provided recommended actions to mitigate these risks down to an acceptable level.
- Actioned as soon as reasonably practicable



PIA Steps

- 12 steps that lead up to a executive management report and presentation
- Not a trivial process but only really requires common sense

1. **Check Compliance with the Privacy Act**
2. **Threshold Assessment**
3. **Plan and Scope the PIA**
4. **Information Gathering**
5. **Information Flow Map Diagram**
6. **Determine the Risks**
7. **Analyse the Risks**
8. **Check Legal Compliance**
9. **Formulate Recommendations**
10. **Prepare the PIA Report**
11. **Present your Results**
12. **Follow up the PIA, document and secure**

Steps to the PIA report (forms and documentation)

Complete Questionnaire:

Does your business need to comply with the Privacy Act?

Do you need to comply with the Privacy Act?

YES

Is a PIA necessary for this project?

YES planning to proceed

Complete Threshold Assessment Checklist

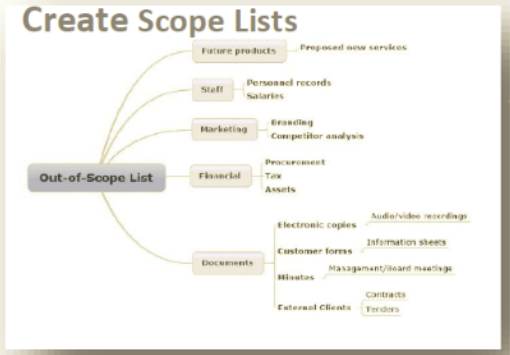
Commence Steps for the PIA Checklist

Plan the PIA—what is in-scope and out-of-scope?

List of essential documents

More documents identified

Create Scope Lists



What information do I need?

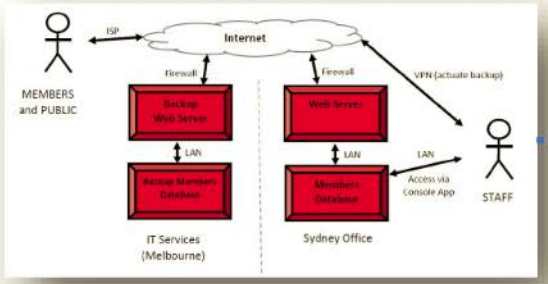
Complete Information needed for the PIA Checklist

Required information identified

Create **Information Flow Map**

Map the Information Flows

All information defined



Feedback from stakeholders

Complete **Key Questions Checklist**

Define and Analyse the Risks

Fill in **Risk Analysis Spreadsheet**

Risks determined

RISK ID	RISK	LIKELIHOOD	IMPACT	RISK VALUE	RISK LEVEL
1	Unresolved security faults that could permit data breaches due to lack of access to good system documentation	LIKELY	MAJOR	16	HIGH
APPLICABLE AUSTRALIAN PRIVACY PRINCIPLES:					
APP11: Security of personal information					
MITIGATION STRATEGY:					
Ensure third parties have service agreements that regularly supply the company with current documentation of the system.					
RATIONALE:					
It is consider 'Likely' that unresolved security faults and/or poor security and privacy practices could still exist. Documentation supplied as part of this PIA have identified access points that have not been covered by previous Penetration Tests. The impact is considered 'Major' since such faults could expose the 'Members' Database. If the entire database was breached through this means it would be 'Catastrophic'. Either way, the risk level would still be evaluated as 'High'.					

More risks identified

Complete **APP Compliance Checklist**

Check Legal Compliance

Non-compliance and compliance identified

Formulate the Recommendations

Complete **Risk Analysis Spreadsheet**

All documented maps, lists and tables collated .

Prepare the PIA report

RECOMMENDATIONS:

The company, preferably through an independent party and not the current sup
understanding of the IT systems in use. A policy supported by service agreemen
most current copies are supplied to and kept by the business. The current list di
inadequate. Obtaining a full set of documents will provide greater independenc
Security audits by the business.

Executive Summary, Project Description, Maps, Checklists, Risk Tables, Compliance and Recommendations.

steps checklist

No.	STEP	Examples and Explanations	Requirements	In Progress	Completed
1	**Check Compliance with the Privacy Act**	Read WHO needs to comply with the Privacy Act? Complete Questionnaire: **'Does your business need to comply with the Privacy Act?'**	☑	☑	☑
2	**Threshold Assessment**	Read WHO needs to do a PIA? Complete the **'Threshold Assessment checklist'** (10 questions)	☑	☑	☑
3	**Plan and Scope the PIA**	Read WHAT do I need to do to plan and scope my PIA? Estimate the size of your PIA then generate **Scope Lists**	☑	☑	☑
4	**Information Gathering**	Read WHAT information will I need? Complete: **'Information needed for the PIA Checklist'** (65 questions)	☑	☑	☑
5	**Information Flow Map Diagram**	Read HOW do I generate an Information Flow Map diagram? Generate your own information maps	☑	☑	☑

step 2 - PIA threshold assessment

threshold outcome

Q9: Who will be involved in the PIA if it goes ahead?

The CEO, two members of the board (one who specializes in IT), the membership manager and a small focus group of volunteer members.

The PIA will be undertaken by the membership manager who currently handles any privacy inquiries.

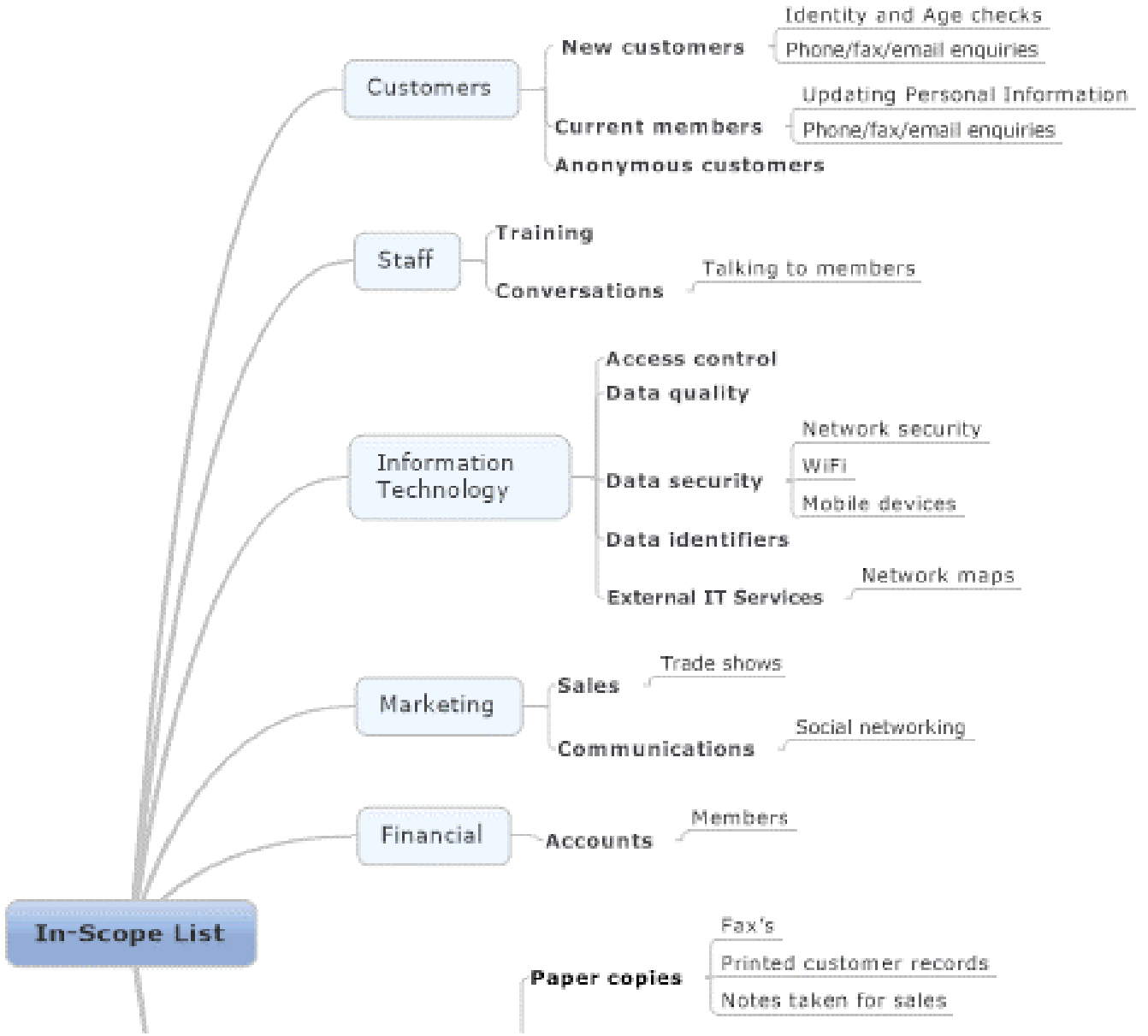
All staff, including sub-contractors will be available for interviews.

Q10: Based on the above answers are you going to proceed to undertake a PIA?

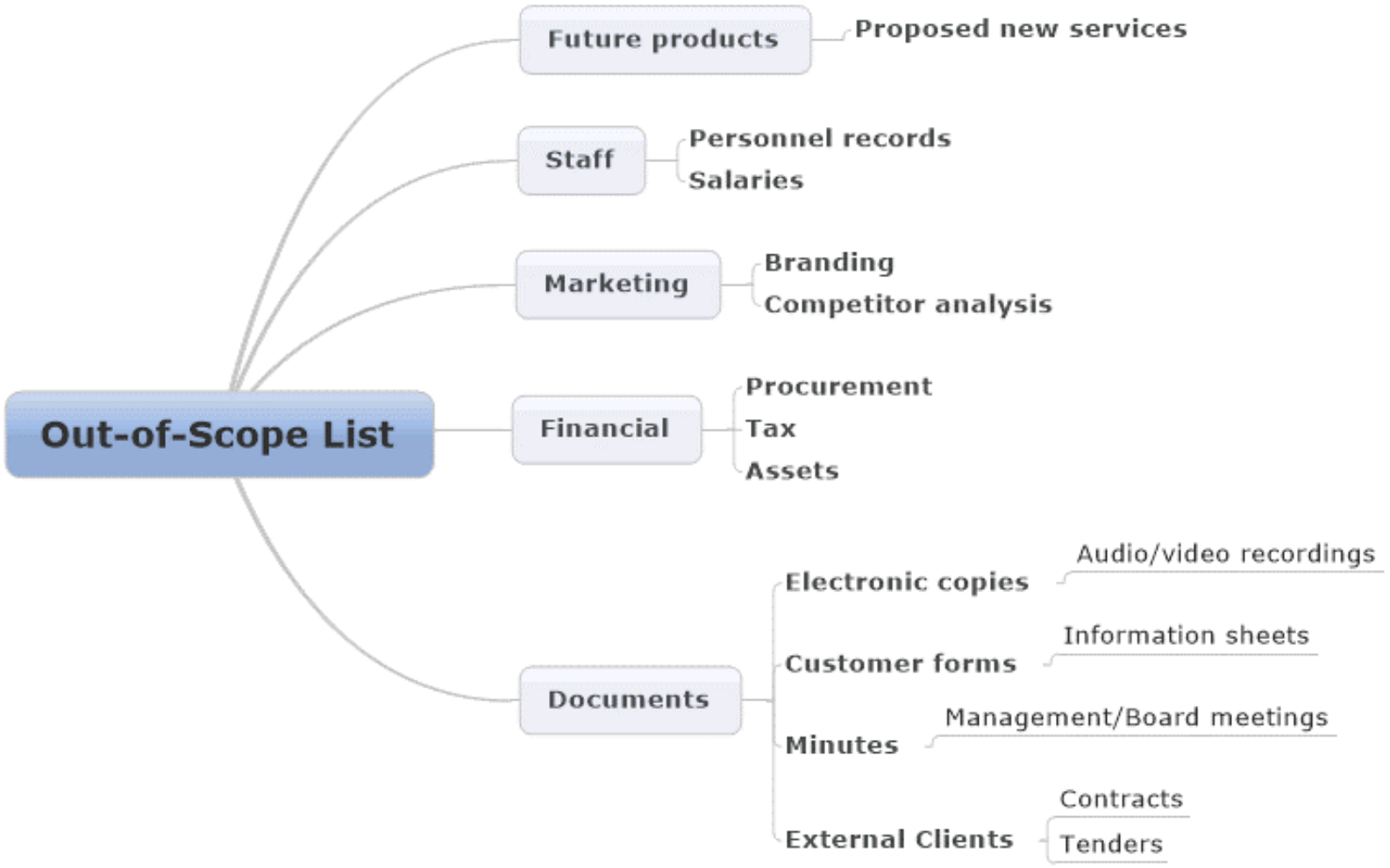
- ( ) NO
- (•) YES
- ( ) UNSURE

- Sensitive information is involved.
- New risks will result from adopting on-line access of personal information.
- Concerns have already been raised by the board of directors and by the current members once this project allows connectivity via the Internet.
- The service has a high public interest profile that demands high privacy protections.
- The cost of undertaking the PIA will be offset by reduced liability insurance costs.

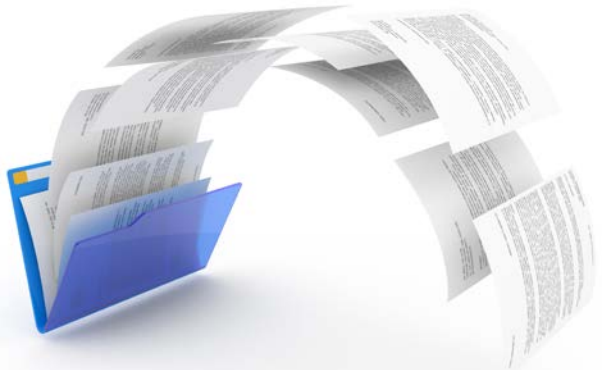
step 3 – scope


In-Scope List
Customers
New customers
Identity and Age checks
Phone/fax/email enquiries
Current members
Updating Personal Information
Phone/fax/email enquiries
Anonymous customers
Staff
Training
Conversations
Talking to members
Information Technology
Access control
Data quality
Data security
Network security
WiFi
Mobile devices
Data identifiers
External IT Services
Network maps
Marketing
Sales
Trade shows
Communications
Social networking
Financial
Accounts
Members
Paper copies
Fax's
Printed customer records
Notes taken for sales

scope (2)

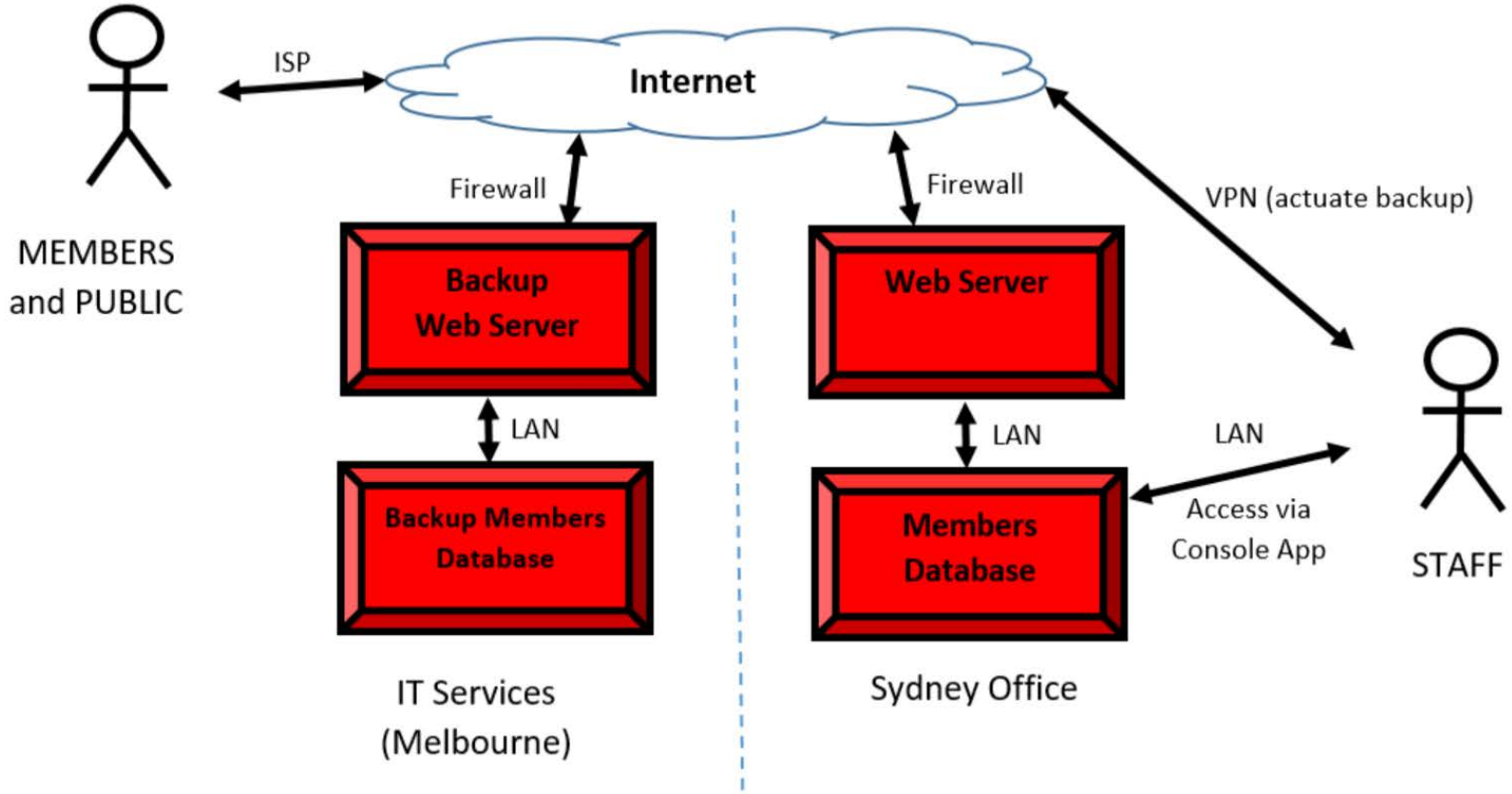

Out-of-Scope List
Future products
Proposed new services
Staff
Personnel records
Salaries
Marketing
Branding
Competitor analysis
Financial
Procurement
Tax
Assets
Documents
Electronic copies
Audio/video recordings
Customer forms
Information sheets
Minutes
Management/Board meetings
External Clients
Contracts
Tenders

step 4 - info needed checklist



No.	1) NECESSITY OF IDENTIFIED VERIFICATION	YES - INFO REQUIRED	NO - NOT APPLICABLE	DONE
1	Can the project can proceed using **anonymous** or **de-identified** data, if so to what extent?	◉	○	☑
	YES partly. This project requires personal information for initial identification and verification of claimed health conditions. Members are encouraged to use suitable pseudonyms when adding comments to the forums.			
2	Is necessary to **verify the identity** of an individual and, if so, to what degree of confidence is needed?	◉	○	☑
	YES. To ensure members are responsible for children with specific health concerns it is necessary to verify their identity with a high degree of confidence. Refer to: 'Members Application Form'			
3	Can you describe the **process** by which the **identity** of individuals will be **verified**?	◉	○	☑
	YES. This will be done using confirmation from a GP or Hospital Refer to: Medical Practitioner's Confirmation Form'			
4	Will **new identification numbers** need to be issued to individuals, and if so, can you describe the purpose of using new IDs and any protections from misuse by others?	○	◉	☐
	NO. Only internal account names.			

step 5 – information mapping



step 6 – determine risks

10 key questions checklist

No.	Key Questions	YES	NO	NOT SURE
1	Do individuals have to give up control of their personal information?	○	◉	○
	NO. Members can modify their information and request that all their personal information is deleted if they leave the service.			
2	Will the project change the way individuals interact with your business, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents?	◉	○	○
	YES. They will now have to use the on-line forms for supplying personal information and updating it. Since the service is already an on-line provision this should not be a problem. Costs will be lower than current postal services. Nothing else changes as individuals must supply identity and health information that is verified by a GP/Hospital.			
3	Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?	○	◉	○
	NO. The decision process on who gets access to the service will be the same.			

step 6 – determine risks

summary of risks table

RISK ID	RISK	LIKELIHOOD	IMPACT	RISK VALUE	RISK LEVEL
1	Unresolved security faults that could permit data breaches due to lack of access to good system documentation	LIKELY	MAJOR	16	HIGH
2	Not updating application software to the latest versions	LIKELY	MAJOR	16	HIGH
3	Staff passwords compromised since they are not strong enough or changed regularly	LIKELY	MAJOR	16	HIGH
4	User allowed to connect own devices (e.g. USB drives)	LIKELY	MAJOR	16	HIGH
5	Disclosure of personal and sensitive information held on shared drives	POSSIBLE	MAJOR	12	MEDIUM
6	System compromised due to web surfing by staff (including temps) while simultaneously having access to database	POSSIBLE	MAJOR	12	MEDIUM
7	Privacy Breach from inadequate incident reporting procedure	POSSIBLE	MAJOR	12	MEDIUM
8	Personal information collected that has no purpose	LIKELY	MODERATE	12	MEDIUM
9	Business identifiers using individual's names	LIKELY	MODERATE	12	MEDIUM

‘Australian Government Protective Security Governance Guidelines’ i.e. business impact levels when determining risk rating

LIKELIHOOD	CONSEQUENCES				
	Insignificant	Negligible	Moderate	Major	Extreme
Remote	VERY LOW	VERY LOW	LOW	MEDIUM	HIGH
Unlikely	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
Possible	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Likely	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Almost certain	LOW	LOW	MEDIUM	HIGH	VERY HIGH

Australian Government publication – ‘Information Security Management Guidelines
Risk management of outsourced ICT arrangements (including Cloud)’

likelihood

The following table shows how to determine the **Likelihood** of an event in a one year period*.

ATTRIBUTE	LIKELIHOOD	EXAMPLE RATIOS
Rare	not expected to ever happen	less than 1 in a 1000 chance
Unlikely	not expected to happen	up to 1 in 100 chance
Possible	could happen	up to 1 in 10 chance
Likely	expected to happen	up to 1 in 1 chance
Almost Certain	will happen	more than a 1 in 1 chance

*(Not that, one year is recommended as the maximum period to coincide with your privacy reviews).

impact

The following table shows how you might determine the **Impact** if the event occurred.

ATTRIBUTE	IMPACT	EXAMPLE COSTS (for SMEs)	EXAMPLE Records Breached
Insignificant	negligible harm to the business	less than $1,000	0
Minor	some harm to the business	up to $5,000	1-4
Moderate	harm the business	up to $25,000	5-99
Major	serious harm to the business	up to $1 million	100-999[!]
Catastrophic	ruin the business	greater than $3M	1,000+[!]

[!]For more sensitive data these numbers could be significantly lower (i.e. use as a guide only)

step 7 – analyse risks

RISK ID	RISK	LIKELIHOOD	IMPACT	RISK VALUE	RISK LEVEL
2	Not updating application software to the latest versions	LIKELY	MAJOR	16	HIGH

APPLICABLE AUSTRALIAN PRIVACY PRINCIPLES:			
APP11: Security of personal information			

MITIGATION STRATEGY:

Ensure all application software is upgraded to include the latest security patches.

RATIONALE:

Adversaries are always looking to exploit vulnerabilities. Security patching is essential to help minimise these risk. Evidence from the PIA showed that such updates only occur following an annual security audits. It is therefore considered 'Likely' that such risks will be exploited and the impact is considered to be 'Major' if not 'Catastrophic' - either will result in an unnecessarily High risk.

RECOMMENDATIONS:

Consult with the IT service providers on more regular updates with patches and the benefits of upgrading to new safer versions when they are made available.

	A	B	C	D	E	G	I	J
1	RISK ID	RISK			LIKELIHOOD	IMPACT	RISK VALUE	RISK LEVEL
2	1						0	
3	APPLICABLE AUSTRALIAN PRIVACY PRINCIPLES:							
4								
5	MITIGATION STRATEGY:							
6								
7	RATIONALE:							
8								
9	RECOMMENDATIONS:							
10								

RISKS | SUMMARY | APPs | RISK MAPPING | TYPICAL RISKS LIST

step 8 – APP compliance

No.	APP1 - open and transparent management of personal information	Examples and Explanations	YES	NEEDS IMPROVING	NOT APPLICABLE
1.1	Does your business have an appropriate **APP compliant Privacy Policy?***	Privacy policy(s) must be clearly expressed, up-to-date, covers the important privacy matters in APP 1.4 and freely available (e.g. on your website).	◉	○	
			Privacy Policy available on the website		
1.2	Have **reasonable steps** been taken that will ensure **compliance with the APPs**?	Evidence the business exercises good practices, procedures and systems for ongoing privacy protection (include APP codes such as credit reporting).	○	◉	
			Identified Risks #7, 18		
1.3	Have **reasonable steps** been taken for handling privacy inquiries and **complaints**?	Evidence the business has in place appropriate complaint procedures and systems	◉	○	
			as per Privacy Policy		

*Note, the eBook: "**Privacy Policy Essentials for Australian Businesses**" covers these requirements in detail.

No.	APP2 - anonymity and pseudonymity	Examples and Explanations	YES	NEEDS IMPROVING	NOT APPLICABLE
2.1	Will individuals participating in the project have the option of **not identifying** themselves?	E.g. when circumstances permit, they will be allowed to remain anonymous OR use a pseudonym (another name)	○	○	◉
			They must identify themselves to join		

step 9 & 10 – Generate Management Recommendations and Report

The PIA should contain two types of recommendations:

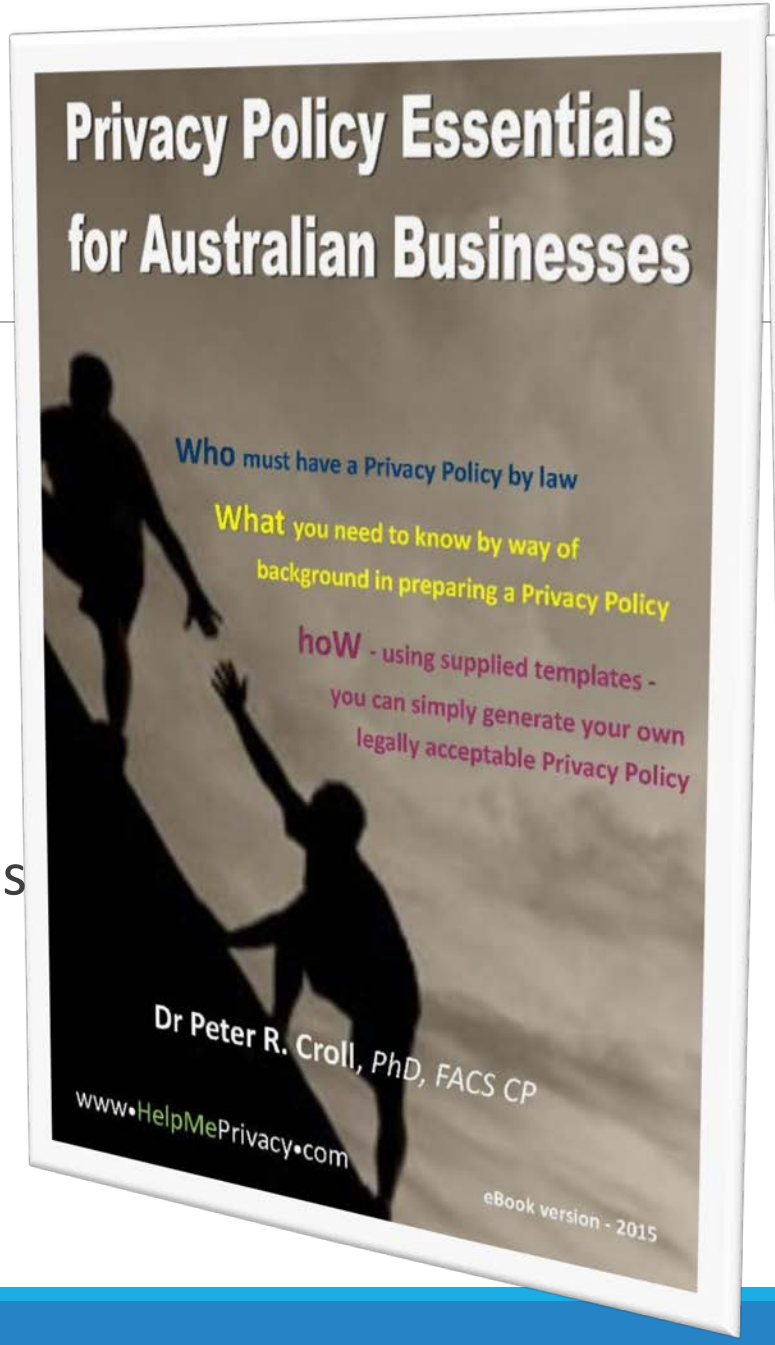
- How to mitigate against each identified risk
- What actions should be taken to progress this project

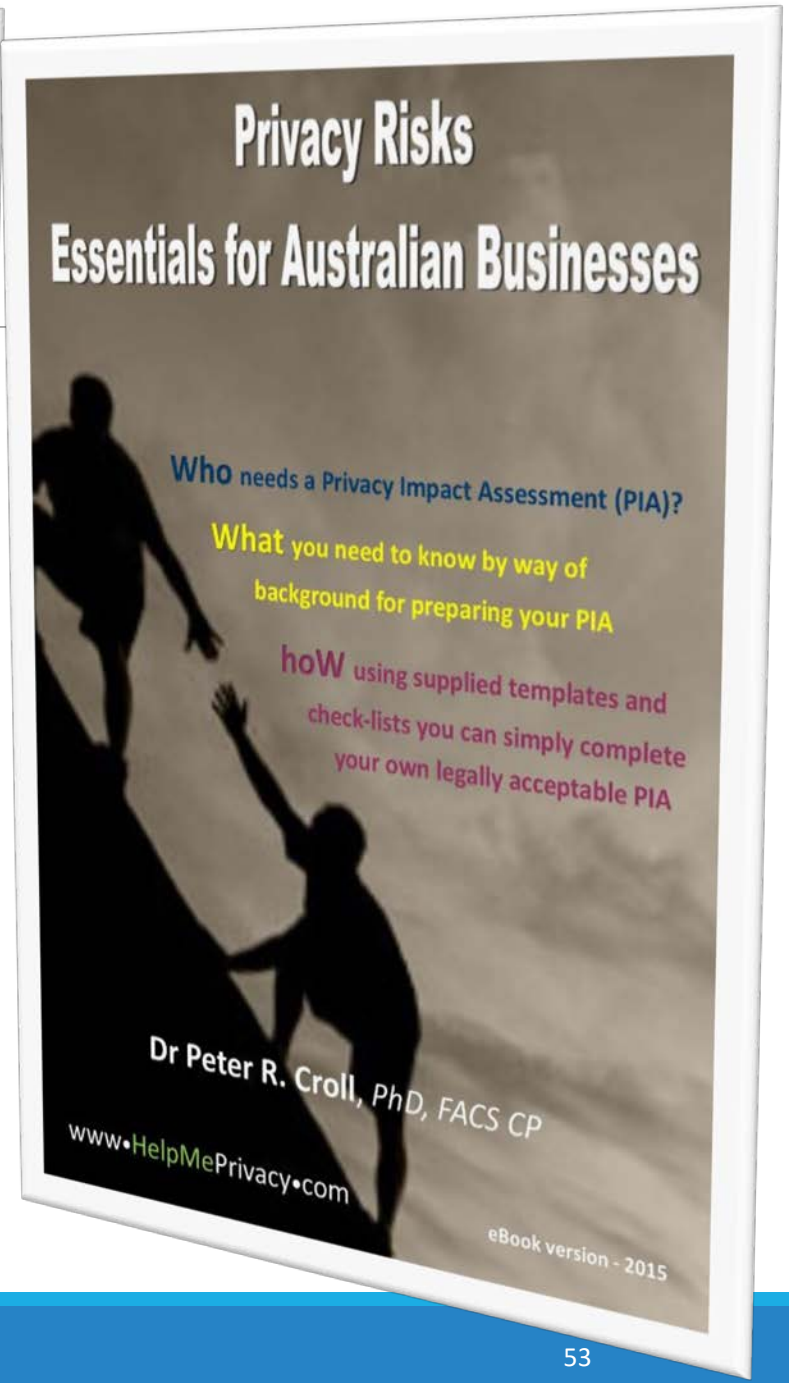
REPORT:

- Title Pages
- Executive Summary
- Approach
- Project Description
- Analysis
- Compliance Check
- Conclusions
- Appendix

Length	Type
2-3 Pages	Threshold Assessment Only
3-15 pages	Brief PIA
15-30 pages	Concise PIA
30-75 pages	Comprehensive PIA
75-150 pages	Detailed PIA
150 pages + (excluding appendices)	Very detailed PIA

- Free samples available
- Contains all the checklists
- Non technical jargon
- Aimed at Australian businesses

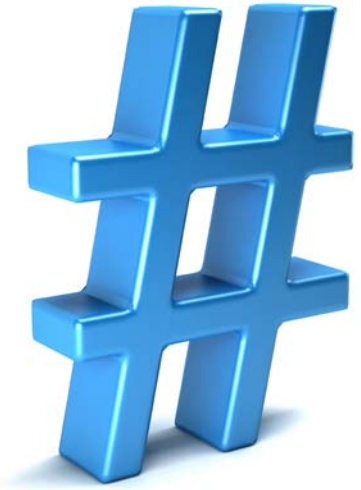




www.HelpMePrivacy.com

topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- **privacy-by-design**
- ‘My Health Record’
- social networking
- the way forward?



privacy by design

An approach when developing a new product or service to ensure that privacy protections have been embedded into all the design stages rather than being added on as an afterthought

The company wanted to comply with APP 10 (Quality) and APP 13 (Correction)

They distributed annually (by post) a copy of the information held on each registered customer

As they grew they found it necessary to use a third party printer who used a mailing company

Following a publicised breach they acted to reduce the risks

To meet monthly deadlines the printer required a CSV file to be sent by FTP

PROBLEM – how could they separate the sensitive information from the customer's name and mailing address if it was being printed?

SOLUTION – ask customers to log-in with password and check/modify their information online.

new problems

Not all customers were comfortable with online access

Most had not previously set up online accounts and – reluctant, just for supplying updates.

Many customers ended up phoning the company - very resource intensive.

Others asked for their details to be posted to them

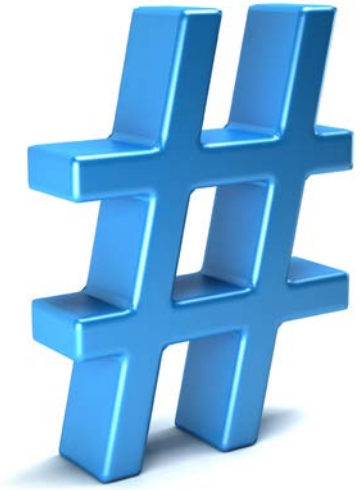
The company ended up with a hybrid solution – new software specifically developed for:

- customers' online access
- separately printing names and addresses labels
- separately printing sensitive information
- auto encryption of the CSV files
- plus extensions to their CRM software

If these privacy concern had been identified and addressed at the design stage their risks and costs would have been significantly reduced.

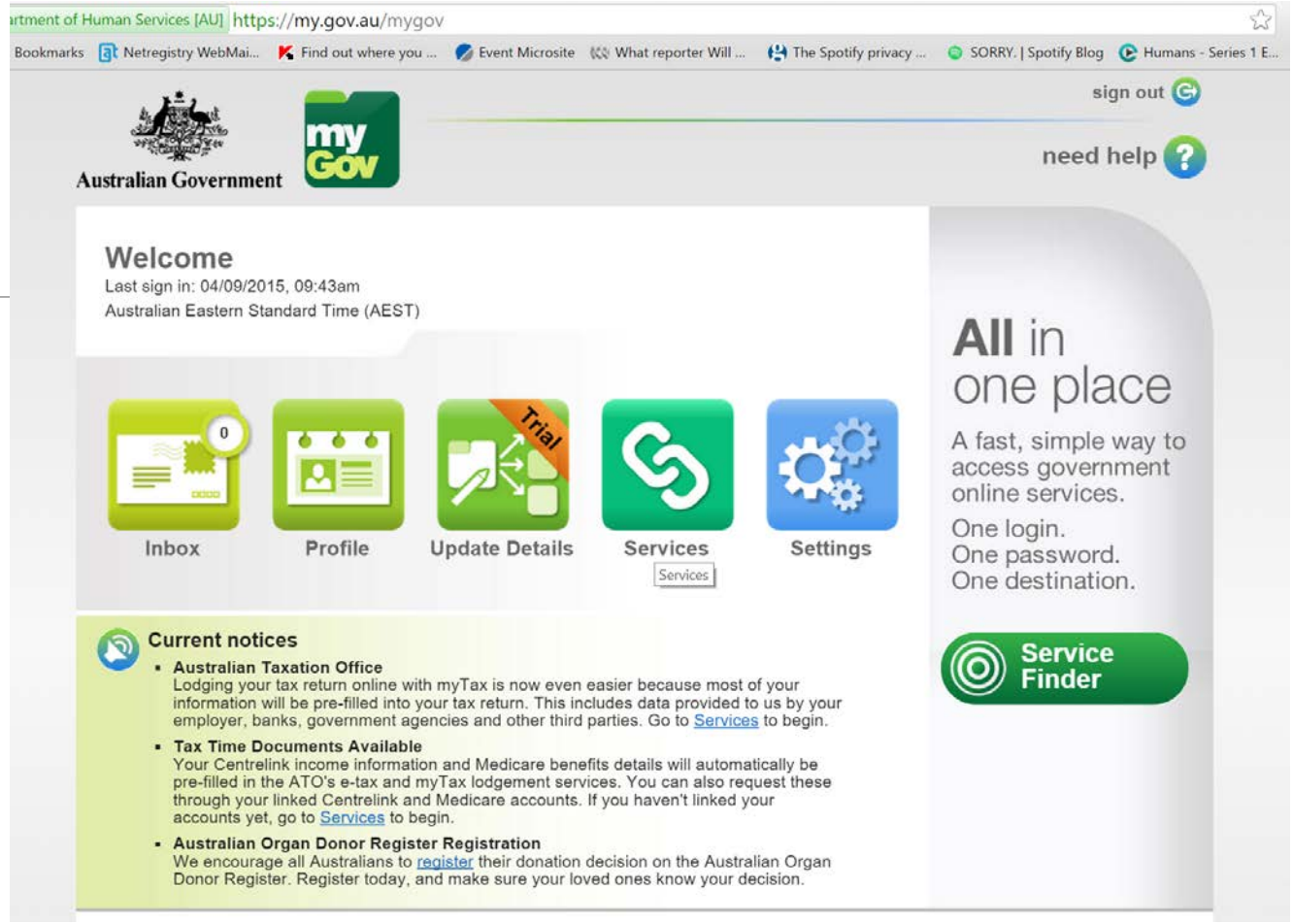
topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- **‘My Health Record’**
- social networking
- the way forward?



‘my Gov’ Services

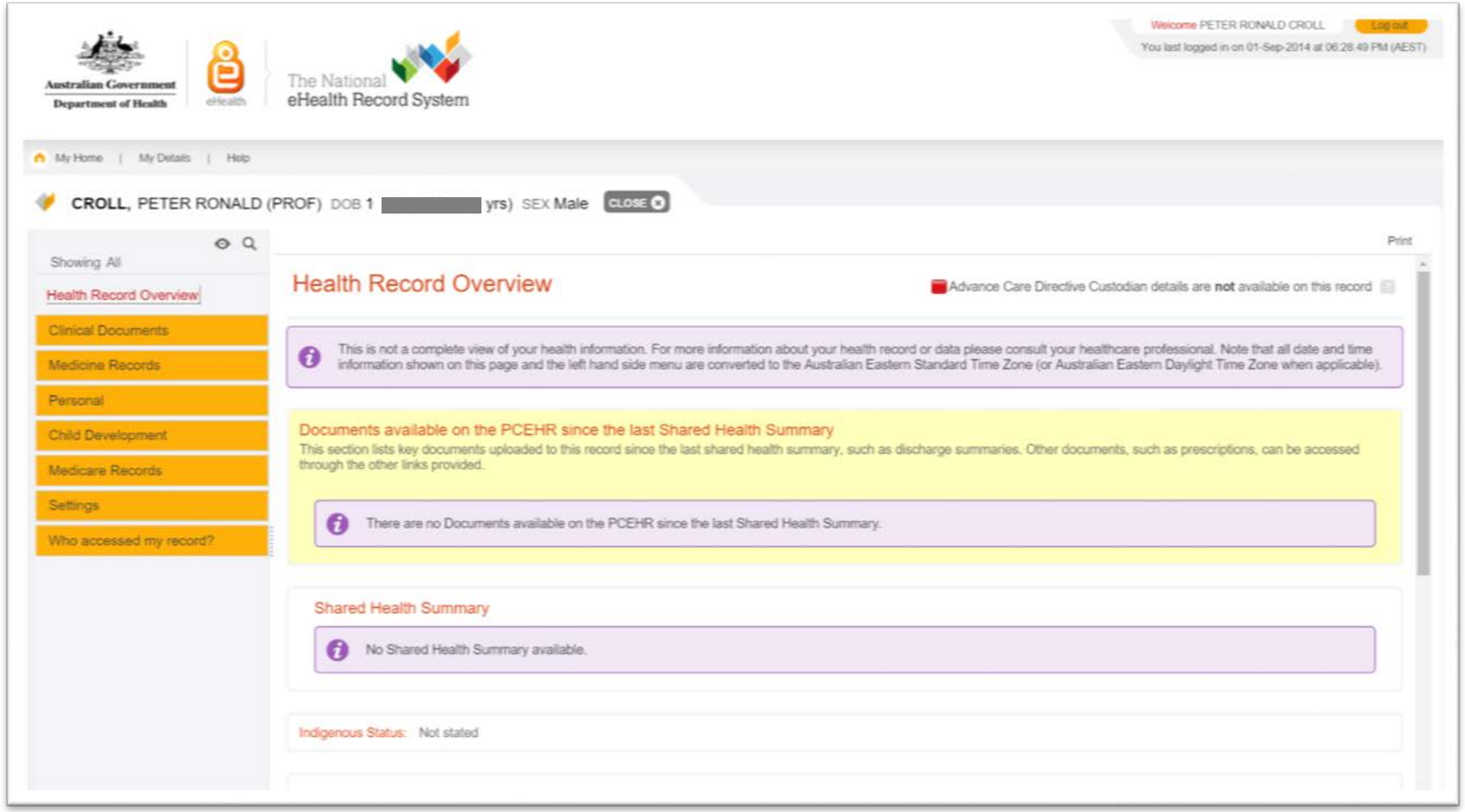
- Medicare
- Centrelink
- Australia Tax Office
- Dept. Veterans Affaires
- My Aged Care
- Child Support
- Nat Disability Ins Service
- Australian Job Search

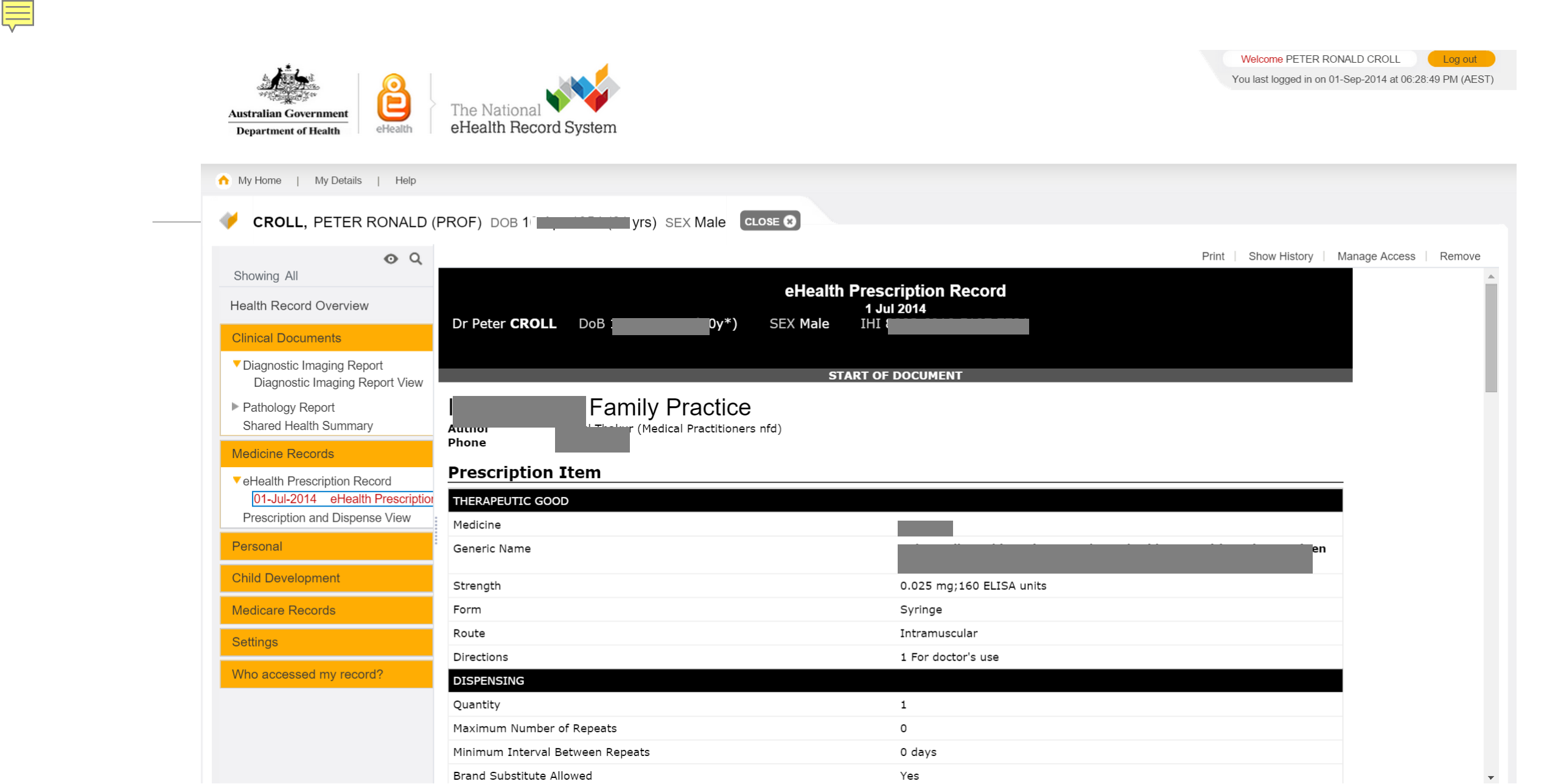


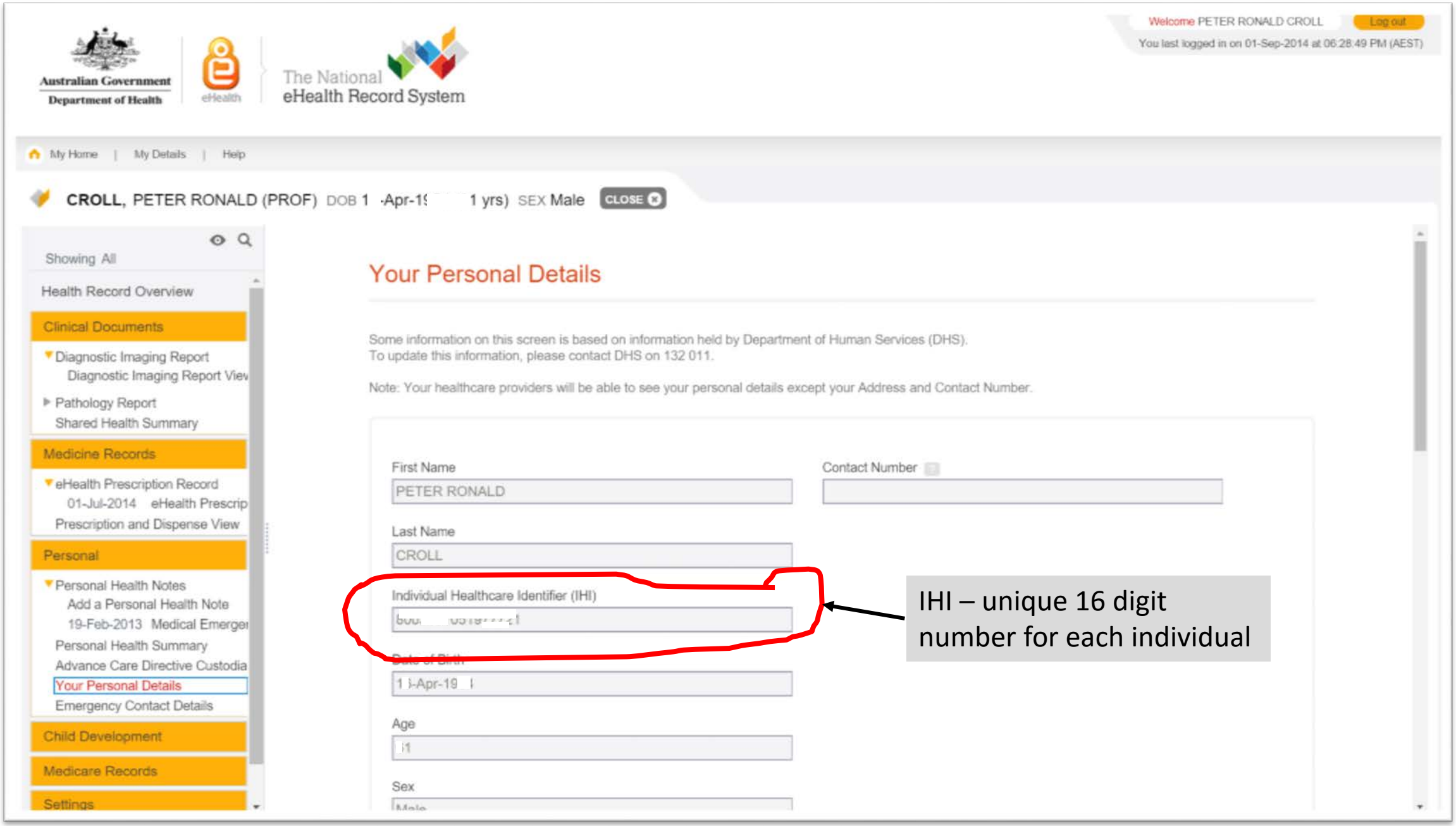
Personally Controlled Electronic Health Record

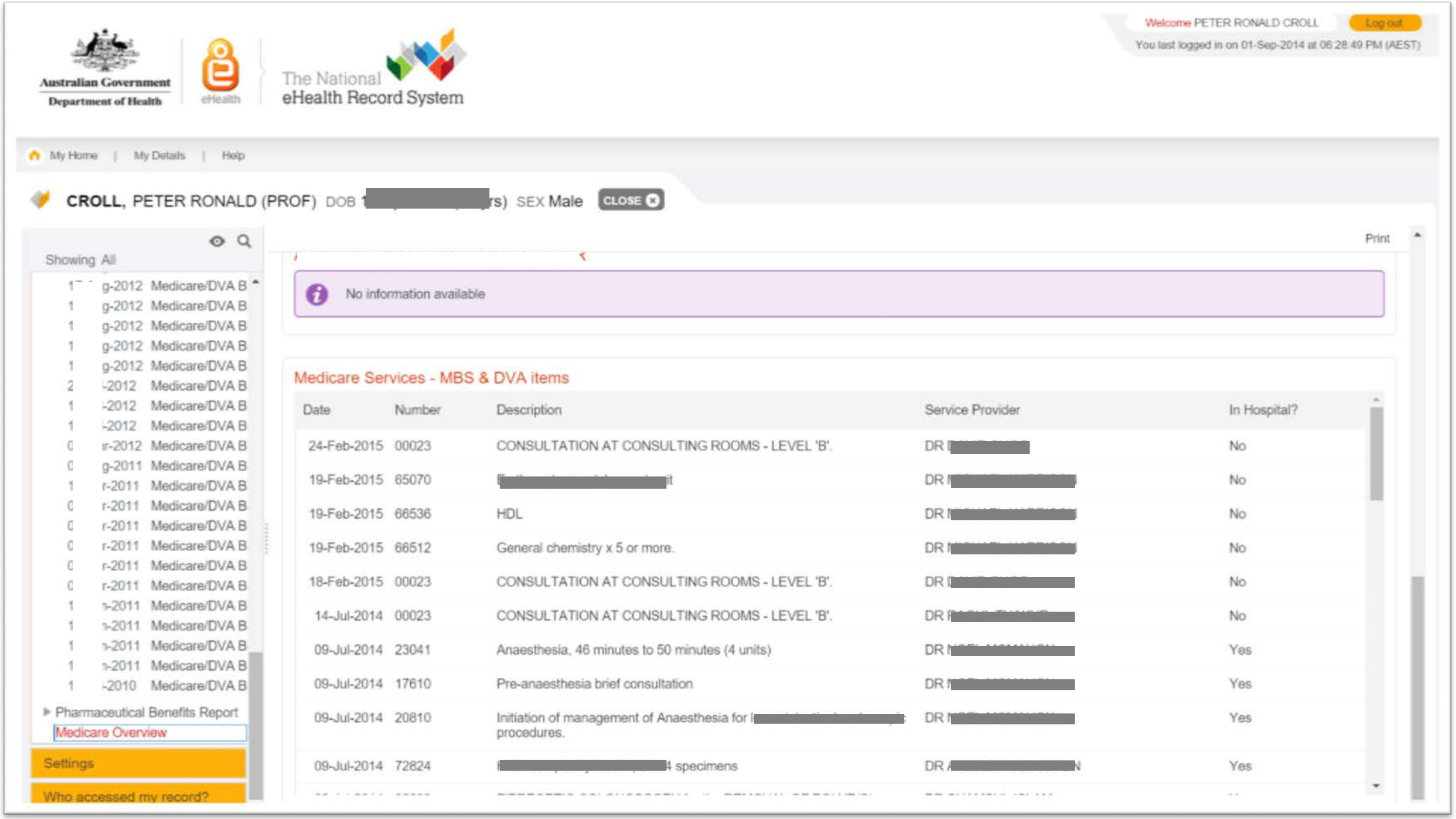
‘My Health Record’

(formally: Personally Controlled Electronic Health Record)

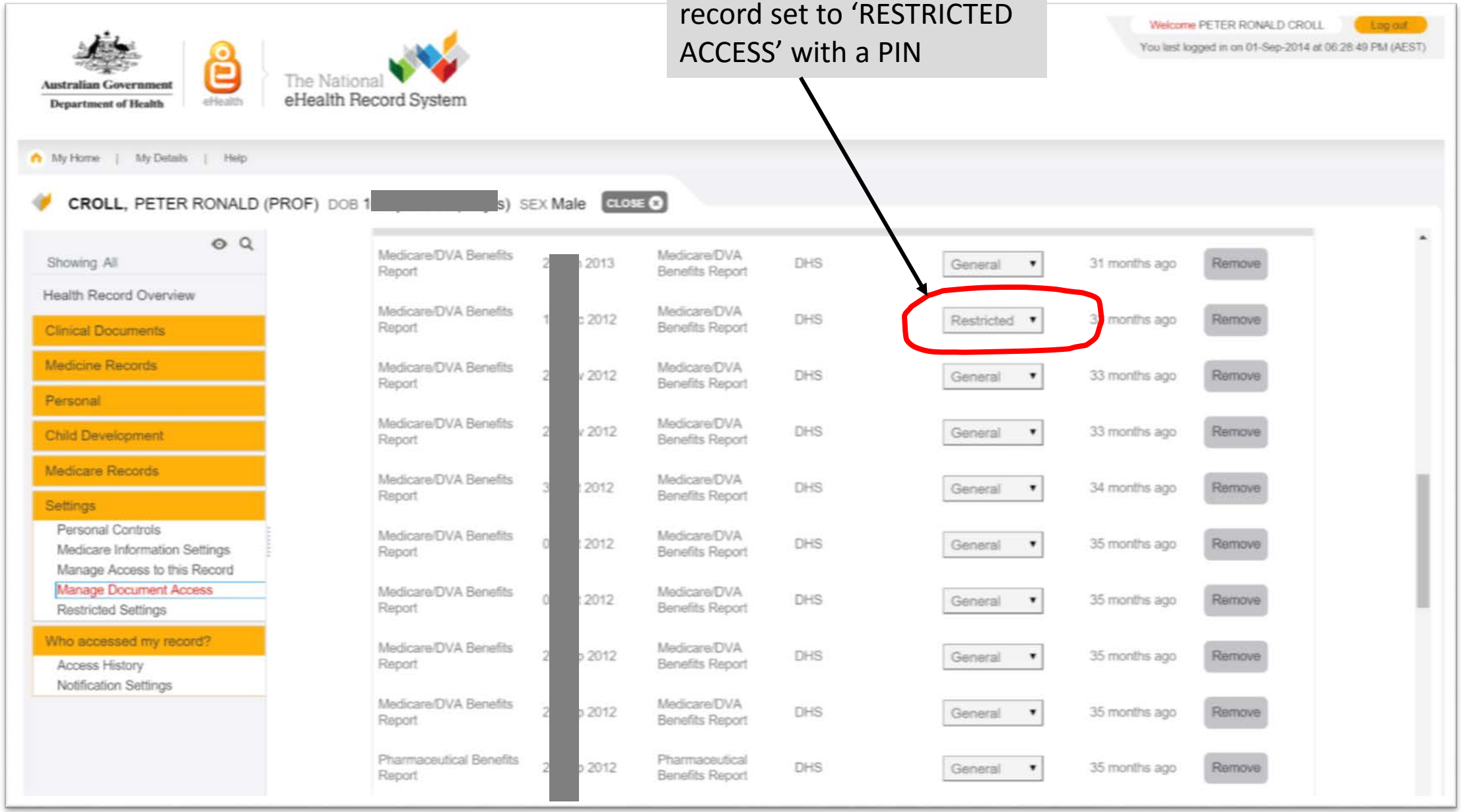


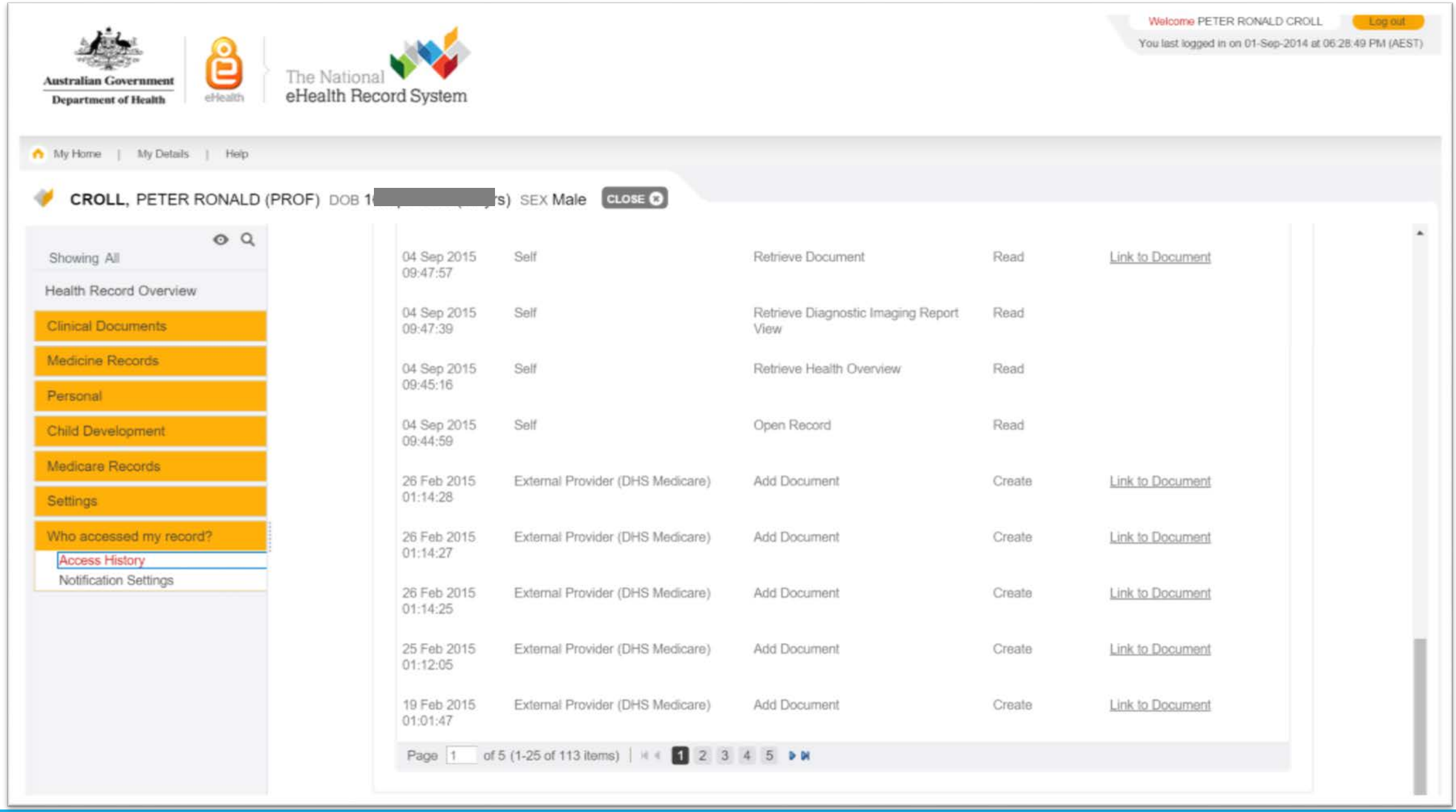

Australian Government
Department of Health
eHealth
The National
eHealth Record System
Welcome PETER RONALD CROLL
Log out
You last logged in on 01-Sep-2014 at 06:28:49 PM (AEST)
My Home | My Details | Help
CROLL, PETER RONALD (PROF) DOB 1 yrs) SEX Male
CLOSE
Showing All
Health Record Overview
Clinical Documents
Diagnostic Imaging Report
Diagnostic Imaging Report View
Pathology Report
Shared Health Summary
Medicine Records
eHealth Prescription Record
01-Jul-2014 eHealth Prescriptio
Prescription and Dispense View
Personal
Child Development
Medicare Records
Settings
Who accessed my record?
Print | Show History | Manage Access | Remove
eHealth Prescription Record
1 Jul 2014
Dr Peter CROLL DoB 0y*) SEX Male IHI
START OF DOCUMENT
Family Practice
(Medical Practitioners nfd)
Phone
Prescription Item
THERAPEUTIC GOOD
Medicine
Generic Name
Strength 0.025 mg;160 ELISA units
Form Syringe
Route Intramuscular
Directions 1 For doctor's use
DISPENSING
Quantity 1
Maximum Number of Repeats 0
Minimum Interval Between Repeats 0 days
Brand Substitute Allowed Yes

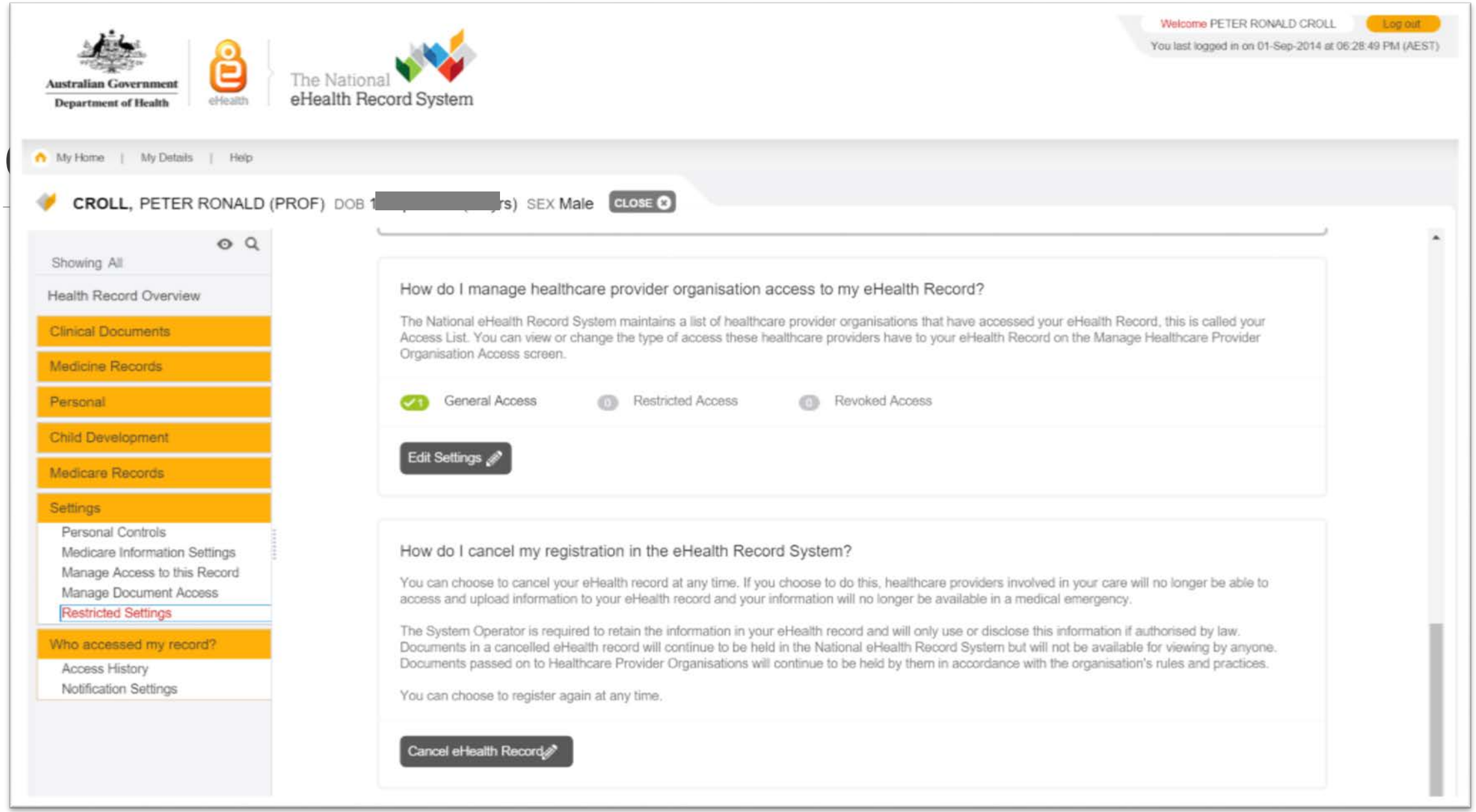

Australian Government
Department of Health
eHealth
The National
eHealth Record System
Welcome PETER RONALD CROLL
Log out
You last logged in on 01-Sep-2014 at 06:28:49 PM (AEST)
My Home | My Details | Help
CROLL, PETER RONALD (PROF) DOB 1 -Apr-19 1 yrs) SEX Male
CLOSE
Showing All
Health Record Overview
Clinical Documents
Diagnostic Imaging Report
Diagnostic Imaging Report Viev
Pathology Report
Shared Health Summary
Medicine Records
eHealth Prescription Record
01-Jul-2014 eHealth Prescrip
Prescription and Dispense View
Personal
Personal Health Notes
Add a Personal Health Note
19-Feb-2013 Medical Emerge
Personal Health Summary
Advance Care Directive Custodia
Your Personal Details
Emergency Contact Details
Child Development
Medicare Records
Settings
Your Personal Details
Some information on this screen is based on information held by Department of Human Services (DHS).
To update this information, please contact DHS on 132 011.
Note: Your healthcare providers will be able to see your personal details except your Address and Contact Number.
First Name
PETER RONALD
Contact Number
Last Name
CROLL
Individual Healthcare Identifier (IHI)
Age
Sex
IHI – unique 16 digit number for each individual


Australian Government
Department of Health
eHealth
The National
eHealth Record System
Welcome PETER RONALD CROLL
Log out
You last logged in on 01-Sep-2014 at 06:28:49 PM (AEST)
My Home | My Details | Help
CROLL, PETER RONALD (PROF) DOB
SEX Male
CLOSE
Print
Showing All
Pharmaceutical Benefits Report
Medicare Overview
Settings
Who accessed my record?
No information available
Medicare Services - MBS & DVA items
Date
Number
Description
Service Provider
In Hospital?
24-Feb-2015 00023 CONSULTATION AT CONSULTING ROOMS - LEVEL 'B'. No
19-Feb-2015 65070 No
19-Feb-2015 66536 HDL No
19-Feb-2015 66512 General chemistry x 5 or more. No
18-Feb-2015 00023 CONSULTATION AT CONSULTING ROOMS - LEVEL 'B'. No
14-Jul-2014 00023 CONSULTATION AT CONSULTING ROOMS - LEVEL 'B'. No
09-Jul-2014 23041 Anaesthesia, 46 minutes to 50 minutes (4 units) Yes
09-Jul-2014 17610 Pre-anaesthesia brief consultation Yes
09-Jul-2014 20810 Initiation of management of Anaesthesia for procedures. Yes
09-Jul-2014 72824 specimens Yes

record set to ‘RESTRICTED ACCESS’ with a PIN




Australian Government
Department of Health
eHealth
The National
eHealth Record System
Welcome PETER RONALD CROLL
Log out
You last logged in on 01-Sep-2014 at 06:28:49 PM (AEST)
My Home | My Details | Help
CROLL, PETER RONALD (PROF) DOB 1
s) SEX Male
CLOSE
Showing All
Health Record Overview
Clinical Documents
Medicine Records
Personal
Child Development
Medicare Records
Settings
Who accessed my record?
Access History
Notification Settings
04 Sep 2015 09:47:57 Self Retrieve Document Read Link to Document
04 Sep 2015 09:47:39 Self Retrieve Diagnostic Imaging Report View Read
04 Sep 2015 09:45:16 Self Retrieve Health Overview Read
04 Sep 2015 09:44:59 Self Open Record Read
26 Feb 2015 01:14:28 External Provider (DHS Medicare) Add Document Create Link to Document
26 Feb 2015 01:14:27 External Provider (DHS Medicare) Add Document Create Link to Document
26 Feb 2015 01:14:25 External Provider (DHS Medicare) Add Document Create Link to Document
25 Feb 2015 01:12:05 External Provider (DHS Medicare) Add Document Create Link to Document
19 Feb 2015 01:01:47 External Provider (DHS Medicare) Add Document Create Link to Document
Page 1 of 5 (1-25 of 113 items)
1 2 3 4 5


Australian Government
Department of Health
eHealth
The National
eHealth Record System
Welcome PETER RONALD CROLL
Log out
You last logged in on 01-Sep-2014 at 06:28:49 PM (AEST)
My Home | My Details | Help
CROLL, PETER RONALD (PROF) DOB
SEX Male
CLOSE
Showing All
Health Record Overview
Clinical Documents
Medicine Records
Personal
Child Development
Medicare Records
Settings
Personal Controls
Medicare Information Settings
Manage Access to this Record
Manage Document Access
Restricted Settings
Who accessed my record?
Access History
Notification Settings
How do I manage healthcare provider organisation access to my eHealth Record?
The National eHealth Record System maintains a list of healthcare provider organisations that have accessed your eHealth Record, this is called your Access List. You can view or change the type of access these healthcare providers have to your eHealth Record on the Manage Healthcare Provider Organisation Access screen.
General Access
Restricted Access
Revoked Access
Edit Settings
How do I cancel my registration in the eHealth Record System?
You can choose to cancel your eHealth record at any time. If you choose to do this, healthcare providers involved in your care will no longer be able to access and upload information to your eHealth record and your information will no longer be available in a medical emergency.
The System Operator is required to retain the information in your eHealth record and will only use or disclose this information if authorised by law. Documents in a cancelled eHealth record will continue to be held in the National eHealth Record System but will not be available for viewing by anyone. Documents passed on to Healthcare Provider Organisations will continue to be held by them in accordance with the organisation's rules and practices.
You can choose to register again at any time.
Cancel eHealth Record

How do I limit access to my eHealth Record?

You may control which healthcare provider organisations access your eHealth Record.

If you wish to specify access for each healthcare provider organisation, you should create a Record Access Code (RAC).

This code will need to be provided to new healthcare providers you want to have access to your eHealth Record.

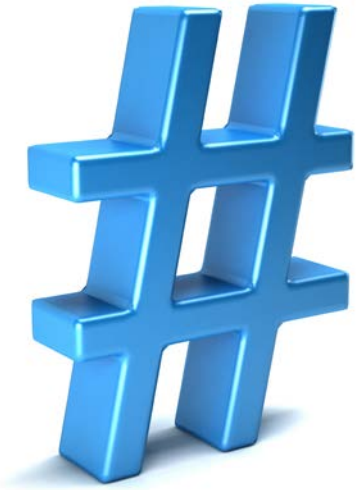
Even if you have a Record Access Code, all information in your record will be available in a medical emergency.

To gain emergency access a healthcare providers must declare that there is a serious threat to your life, health or safety.

If you do not have a Record Access Code, any healthcare providers involved in your care can access your Record.

topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- **social networking**
- the way forward?



Records stored in cloud

No encryption was used

Prior to the new APPs

consider privacy of other Aus dating sites

choice the consumer advocate and product review organisation (www.choice.com.au)

their investigation into popular online dating sites, including RSVP, eHarmony, Oasis Active, Plenty of Fish, Zoosk and OkCupid, and the popular app Tinder

they found that scams are rife, and some privacy policies and terms and conditions are riddled with disturbing provisions

RSVP

Signing up to an RSVP account and agreeing to its privacy terms and conditions in effect grants permission for your personal information, including photos and email addresses, to be used for "any purpose" , which may include advertising or transmission to a third party.

While all sites we looked at track your activities using cookies, RSVP even shows other users how often you're on the site and who you're looking at.

eHarmony

By posting information and photos on a profile page or any public area of the eHarmony website, users automatically agree to have that information perpetually owned and used by eHarmony for purposes such as advertising.

Users' contact details may be shared with third parties for advertising, but opting out is possible by changing certain settings or notifying eHarmony of your request in writing.

Oasis Active

By signing up, users agree that all profile information– including photos – is public, and so automatically grant an irrevocable and ongoing licence for the company to use and distribute any information posted or transmitted on the site.

In effect, this means users' photos, aliases and other personal details can be used in advertising, online and off, although it's possible to opt out of this by updating privacy options in the account settings portal on the website.

Email addresses, photos and information may also be shared with third parties for marketing purposes on behalf of Oasis Active.

OkCupid

OkCupid may use contact information for advertising purposes and compiling its OkTrends blog, which tracks and charts user behaviour.

They may also share this information with third parties.

OkCupid allows information posted on its site to appear in search engine results.

Plenty of Fish (PoF)

PoF says it may share your personal information with affiliates and third parties acting on their behalf in the "normal course of business", though they do say they won't sell it to others.

Tinder

Privacy is a significant concern when it comes to Tinder, as users sign up with their Facebook profile, meaning the company has access to a large amount of personal information, including your email address, likes, birthday, education history, interests, current city, personal description, your friends list, and photos of you and your Facebook friends who might be common with other users.

Tinder also gives itself access to the content of your chats when you're using the app, and uses this information to market itself and third party products or services.

You can't delete your Tinder account, only the app. This means your virtual Tinder footprint could exist in perpetuity.

Zoosk

If you sign up to Zoosk and give the site access to one of your social media profiles, such as Twitter or Facebook, they may make posts on your behalf on that platform.

Think twice about giving Zoosk access to your address book – they keep your contacts on file and may later use your information to suggest friends and connections to other members.

By signing up to Zoosk, you grant permission for all your user content to be used for purposes including advertising or transmission to a third party.

spotify

SORRY.

A blog post by Spotify CEO, Daniel Ek, August 21st, 2015 10:02

We are in the middle of rolling out new terms and conditions and privacy policy and they've caused a lot of confusion about what kind of information we access and what we do with it. We apologize for that. We should have done a better job in communicating what these policies mean and how any information you choose to share will – and will not – be used.

We understand people's concerns about their personal information and are 100 percent committed to protecting our users' privacy and ensuring that you have control over the information you share.

So let me try and clear things up.

In our new privacy policy, we indicated that we may ask your permission to access new types of information, including photos, mobile device location, voice controls, and your contacts. **Let me be crystal clear here: If you don't want to share this kind of information, you don't have to.** We will ask for your express permission before accessing any of this data – and we will only use it for specific purposes that will allow you to customize your Spotify experience.

what you grant to spotify (terms)

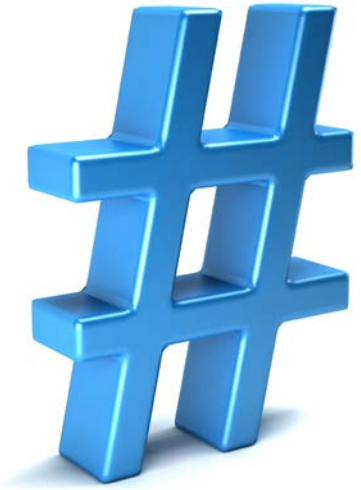
You grant Spotify a non-exclusive, transferable, sub-licensable, royalty-free, perpetual (or, in jurisdictions where this is not permitted, for a term equal to the duration of the Agreements plus twenty (20) years), irrevocable, fully paid, worldwide licence to use, reproduce, make available to the public (e.g. perform or display), publish, translate, modify, create derivative works from, and distribute any of your User Content in connection with the Service through any medium, whether alone or in combination with other content or materials, in any manner and by any means, method or technology, whether now known or hereafter created.

……you also agree to waive any "moral rights" …… and your right to object to derogatory treatment ……

This is not under their Privacy Policy but under their Terms and Conditions of Use – a link from the full Privacy Policy – total of 24 pages – over 8,000 words.

topics

- is privacy dead?
- privacy law changes
- holistic view of privacy
- calculating privacy risks
- privacy analysis – case study
- privacy-by-design
- ‘My Health Record’
- social networking
- **the way forward?**



IMIA's WG 4 'security in health information systems'

- SiHIS seeking to address global inadequacies for many years
- proposals on minimum standards, guidelines, legislative frameworks, voluntary codes, etc.
- have been widely debated and published
- health information protection has previously relied on regulated models that are somewhat static.
- patients seeking '**confidentiality**' place trust in the health professionals who they regard as in control.
- yet, today's connected world is not adequately controlled.
- with digital data, significant measures are required to implement '**Privacy**' protection.

the way forward?

- #1 ensure your organisation is privacy compliant (APPs)
- #2 take a holistic view on privacy
- #3 do a Privacy Impact Assessment (PIA) with all new projects
- #4 follow a ‘Privacy-by-Design’ approach
- #5 report breaches and act promptly to prevent them reoccurring
- #6 don’t sign up to social networks without checking what you’re committing to
- #7 don’t give out any personal information you don’t need to, or want to
- #8 take control of your personal information, whenever possible

Thank You!

w: www.PeterCroll.com
e: help@petercroll.com