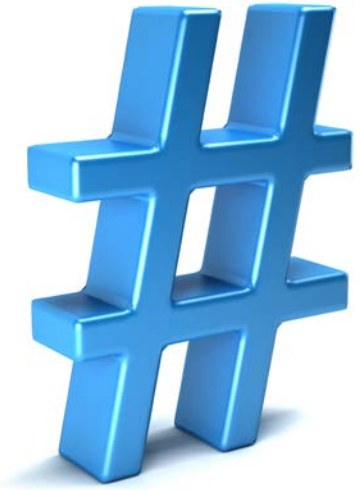
Privacy and Legal framework

- legislative patchwork - what is 'reasonable' - holistic approach

DR PETER R. CROLL

PRC@PETERCROLL.COM

topics



- **legislative patchwork**

  (introduction to Australian legal framework on health information protection)

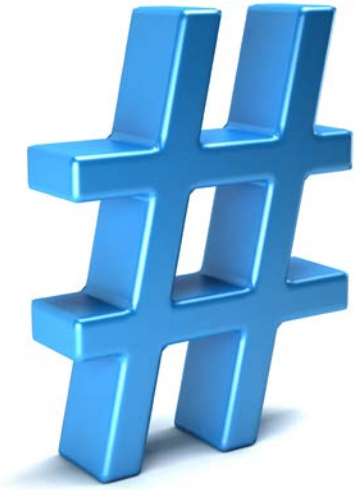
- **what is ‘reasonable’**

  (privacy demands ‘reasonable security’ and confidentiality measures – what does that entail in today’s cyber world)?

- **holistic approach**

  (the necessity to take a holistic view on to minimise privacy risks to acceptable levels)

topics



- **legislative patchwork**

  (introduction to Australian legal framework on health information protection)

- **what is ‘reasonable’**

  (privacy demands ‘reasonable security’ and confidentiality measures – what does that entail in today’s cyber world)?

- **holistic approach**

  (the necessity to take a holistic view on to minimise privacy risks to acceptable levels)

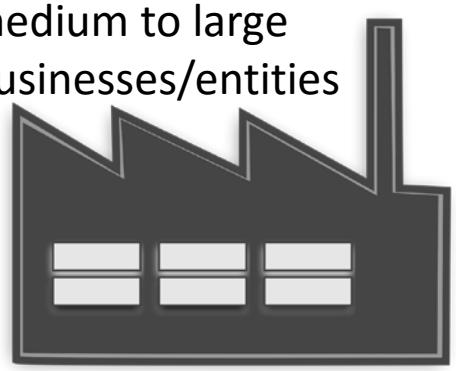
legislative patchwork

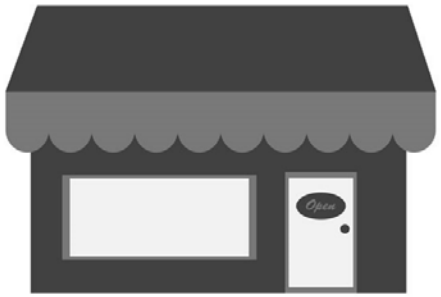
commonwealth

legislative patchwork

commonwealth

medium to large businesses/entities

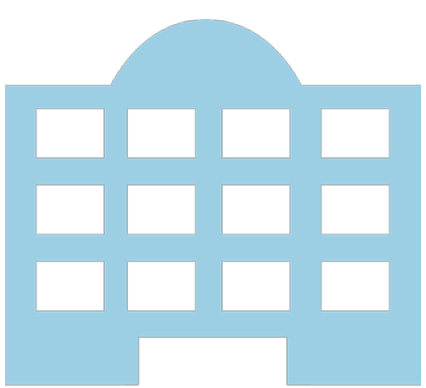


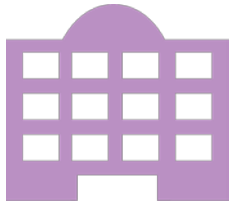


small businesses/entities

legislative patchwork

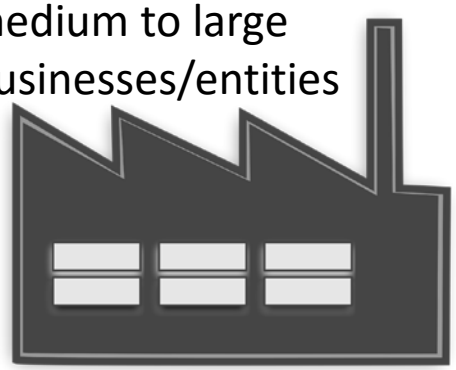
commonwealth

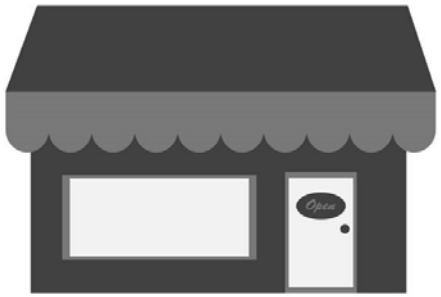




state/territory governments

medium to large businesses/entities





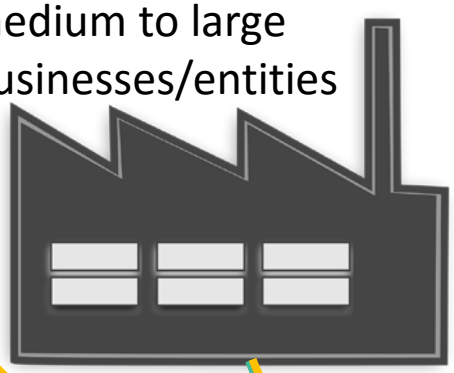
small businesses/entities

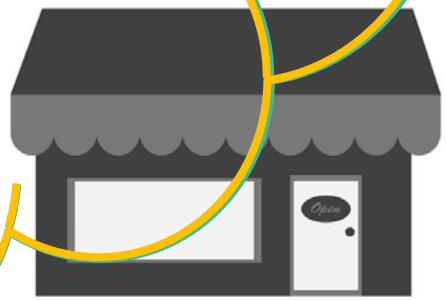
legislative patchwork

The Privacy Act 1988 (Cth)

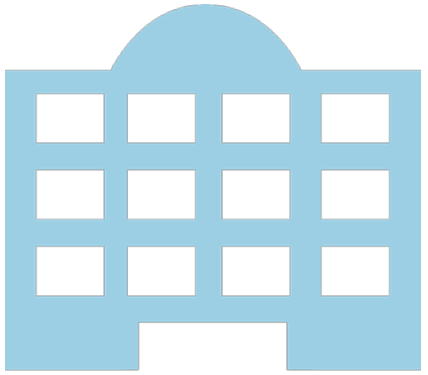
commonwealth

medium to large businesses/entities

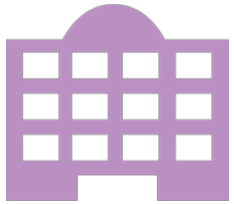




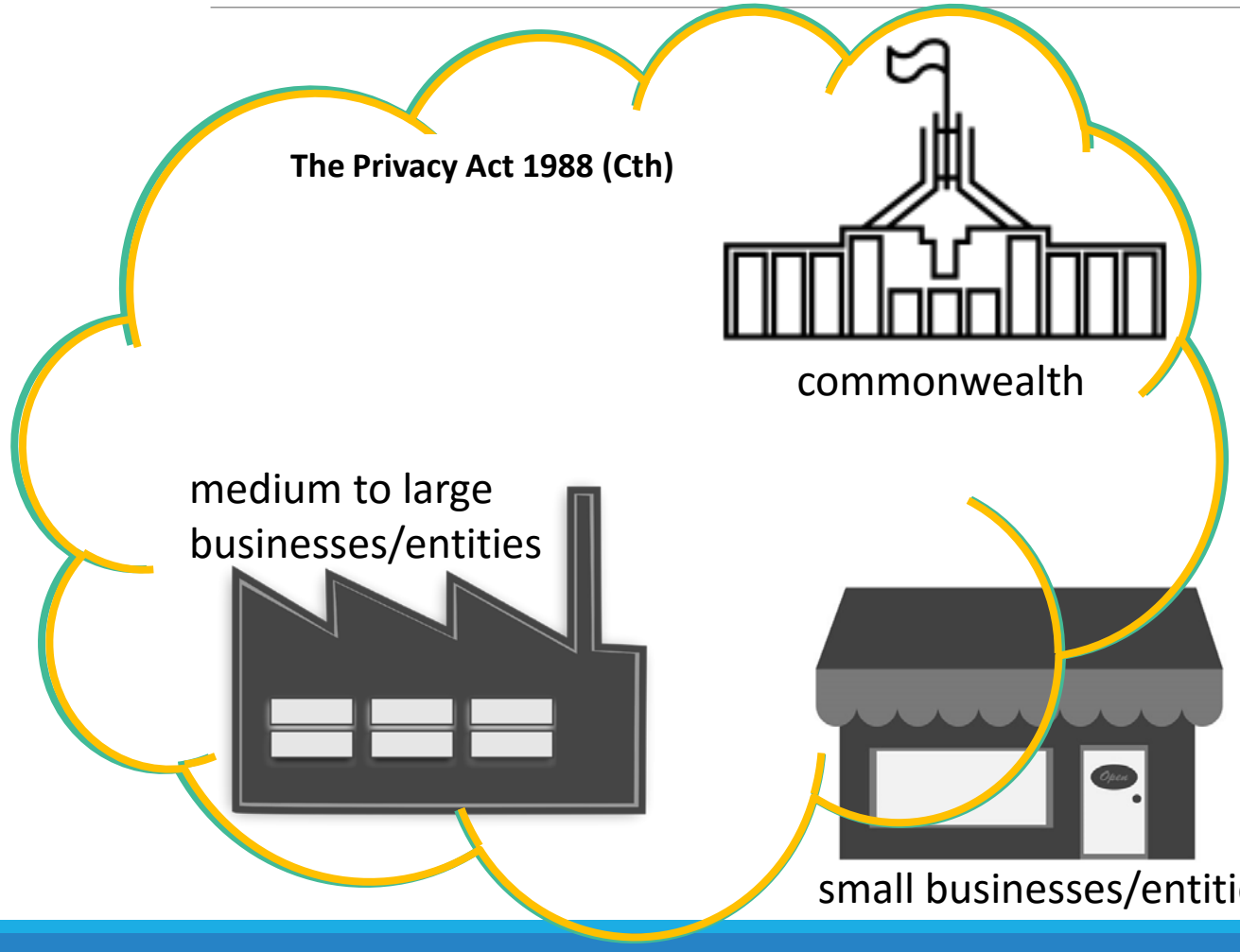
small businesses/entities

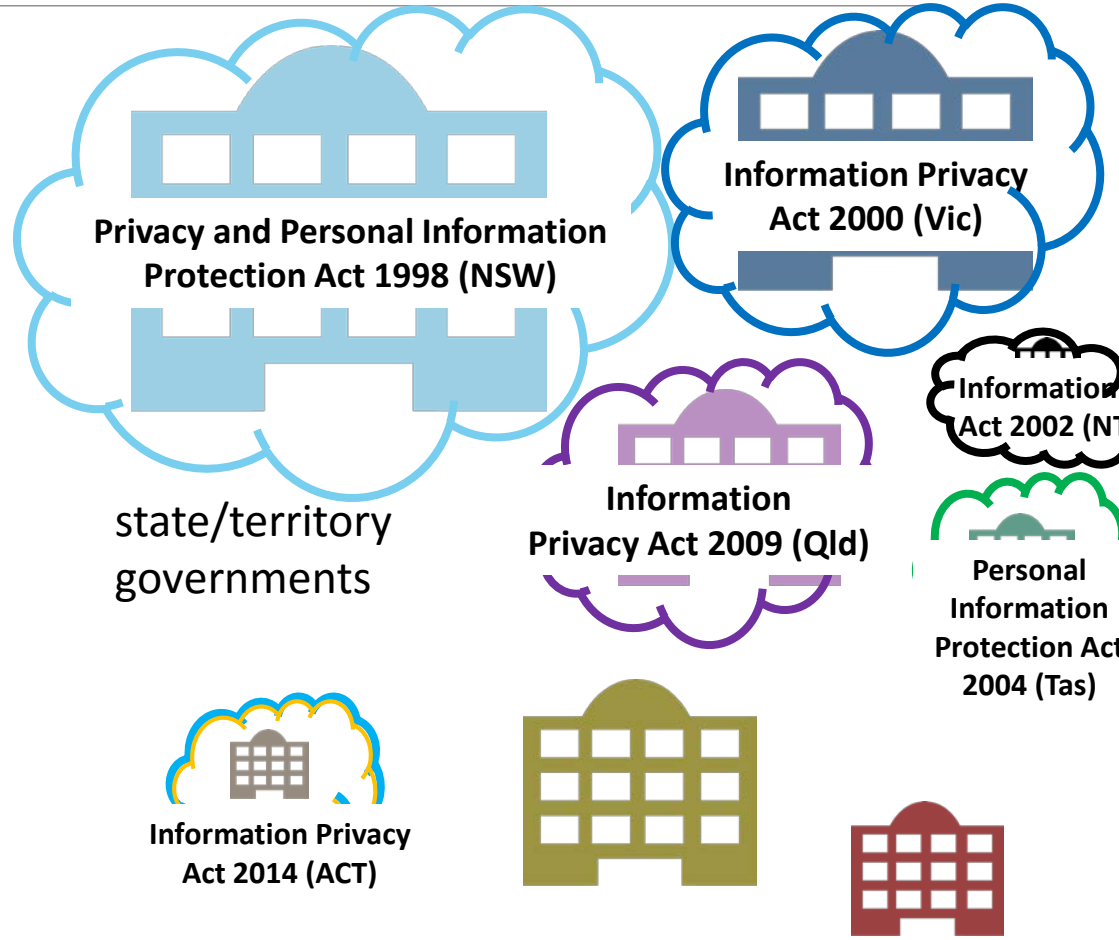


state/territory governments



legislative patchwork



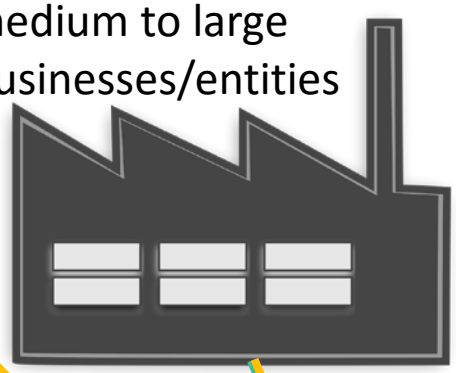


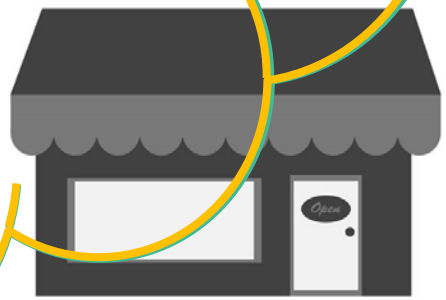
legislative patchwork

The Privacy Act 1988 (Cth)

commonwealth

medium to large businesses/entities





small businesses/entities

Health Records and Information Privacy Regulation 2012 (NSW)

Health Records Act 2001 (Vic)

Drug Court Act 1998 (NSW)

Government Information (Public Access) Act 2009 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2000 (NSW)

Freedom of Information Act 1982 (Vic)

Information Privacy Act 2000 (Vic)

Cancer (Registration) Act 1997 (NT)

Information Act 2002 (NT)

Personal Injuries Proceedings Act 2002 (Qld)

Right to Information Act 2009 (Tas)

state/territory governments

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Hospital and Health Boards Act 2011 (Qld)

Personal Information Protection Act 2004 (Tas)

Public Health Act 1997 (ACT)

Drugs of Dependence Act 1989 (ACT)

Information Privacy Act 2014 (ACT)

Health Records (Privacy and Access) Act 1997 (ACT)

Health Act 1911 (WA)

Freedom of Information Act 1992 (WA)

Public Health Act 1997 (Tas)

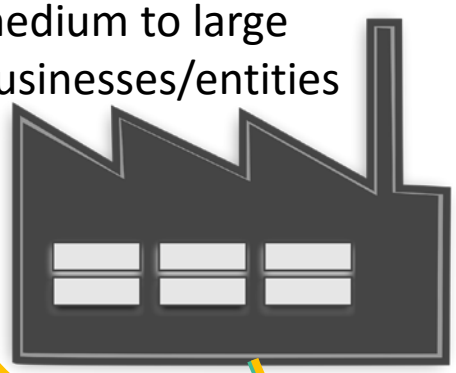
Freedom of Information Act 1991 (SA)

legislative patchwork

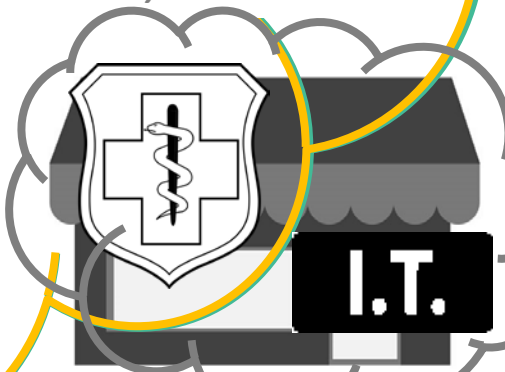
The Privacy Act 1988 (Cth)

commonwealth

medium to large businesses/entities



cover by contract



small businesses/entities

Health Records and Information Privacy Regulation 2012 (NSW)

Health Records Act 2001 (Vic)

Drug Court Act 1998 (NSW)

Government Information (Public Access) Act 2009 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2000 (NSW)

Freedom of Information Act 1982 (Vic)

Information Privacy Act 2000 (Vic)

Cancer (Registration) Act 1997 (NT)

Information Act 2002 (NT)

Personal Injuries Proceedings Act 2002 (Qld)

Right to Information Act 2009 (Tas)

state/territory governments

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Personal Information Protection Act 2004 (Tas)

Hospital and Health Boards Act 2011 (Qld)

Public Health Act 1997 (ACT)

Drugs of Dependence Act 1989 (ACT)

Information Privacy Act 2014 (ACT)

Health Act 1911 (WA)

Freedom of Information Act 1992 (WA)

Public Health Act 1997 (Tas)

Freedom of Information Act 1991 (SA)

Health Records (Privacy and Access) Act 1997 (ACT)

legislative patchwork

The Privacy Act 1988 (Cth)
The Healthcare Identifiers Act 2010 (Cth)
My Health Record Act 2012 (Cth)
Freedom of Information Act (FOIA) 1982 (Cth)

commonwealth

medium to large businesses/entities

cover by contract

small businesses/entities

Health Records and Information Privacy Regulation 2012 (NSW)
Health Records Act 2001 (Vic)
Drug Court Act 1998 (NSW)
Government Information (Public Access) Act 2009 (NSW)
Freedom of Information Act 1982 (Vic)
Information Privacy Act 2000 (Vic)
Privacy and Personal Information Protection Act 1998 (NSW)
Health Records and Information Privacy Act 2000 (NSW)
Cancer (Registration) Act 1997 (NT)
Information Act 2002 (NT)
Personal Injuries Proceedings Act 2002 (Qld)
Right to Information Act 2009 (Tas)
Information Privacy Act 2009 (Qld)
Right to Information Act 2009 (Qld)
Personal Information Protection Act 2004 (Tas)
Hospital and Health Boards Act 2011 (Qld)
Public Health Act 1997 (ACT)
Public Health Act 1997 (Tas)
Drugs of Dependence Act 1989 (ACT)
Health Act 1911 (WA)
Information Privacy Act 2014 (ACT)
Freedom of Information Act 1992 (WA)
Freedom of Information Act 1991 (SA)
Health Records (Privacy and Access) Act 1997 (ACT)

state/territory governments

legislative patchwork

The Privacy Act 1988 (Cth)
The Healthcare Identifiers Act 2010 (Cth)
My Health Record Act 2012 (Cth)

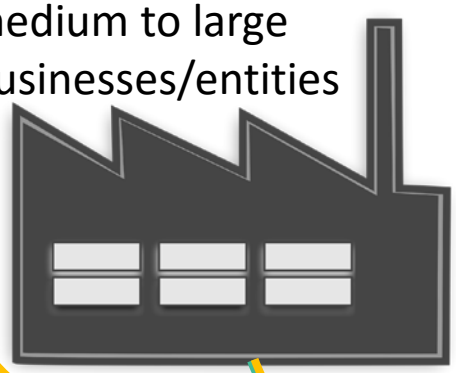
Freedom of Information Act (FOIA) 1982 (Cth)

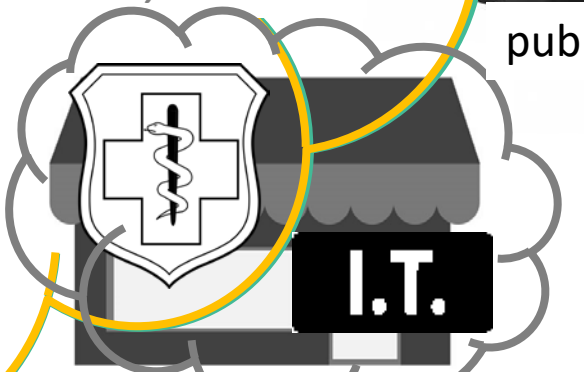
commonwealth

ANU/Bond

cover by contract

medium to large businesses/entities





small businesses/entities

public

state/territory governments

Health Records and Information Privacy Regulation 2012 (NSW)

Drug Court Act 1998 (NSW)

Government Information (Public Access) Act 2009 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2000 (NSW)

Health Records Act 2001 (Vic)

Freedom of Information Act 1982 (Vic)

Information Privacy Act 2000 (Vic)

Cancer (Registration) Act 1997 (NT)

Information Act 2002 (NT)

Personal Injuries Proceedings Act 2002 (Qld)

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Hospital and Health Boards Act 2011 (Qld)

Right to Information Act 2009 (Tas)

Personal Information Protection Act 2004 (Tas)

Public Health Act 1997 (ACT)

Drugs of Dependence Act 1989 (ACT)

Information Privacy Act 2014 (ACT)

Health Records (Privacy and Access) Act 1997 (ACT)

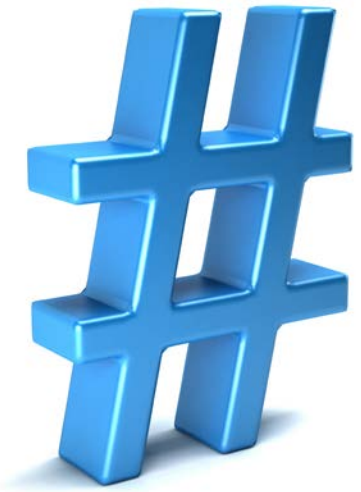
Health Act 1911 (WA)

Freedom of Information Act 1992 (WA)

Public Health Act 1997 (Tas)

Freedom of Information Act 1991 (SA)

topics



- **legislative patchwork**

  (introduction to Australian legal framework on health information protection)

- **what is ‘reasonable’**

  (privacy demands ‘reasonable security’ and confidentiality measures – what does that entail in today’s cyber world)?

- **holistic approach**

  (the necessity to take a holistic view on to minimise privacy risks to acceptable levels)

what is ‘reasonable’

- reasonable appears 155 times in Privacy Act
- is encryption reasonable?
- are cloud services reasonable?
- is it reasonable to store overseas?
- is it reasonable for the cloud service provider to mange the encryption keys?
- is this your problem?

reasonable security

11 Australian Privacy Principle 11—Security of Personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are

reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

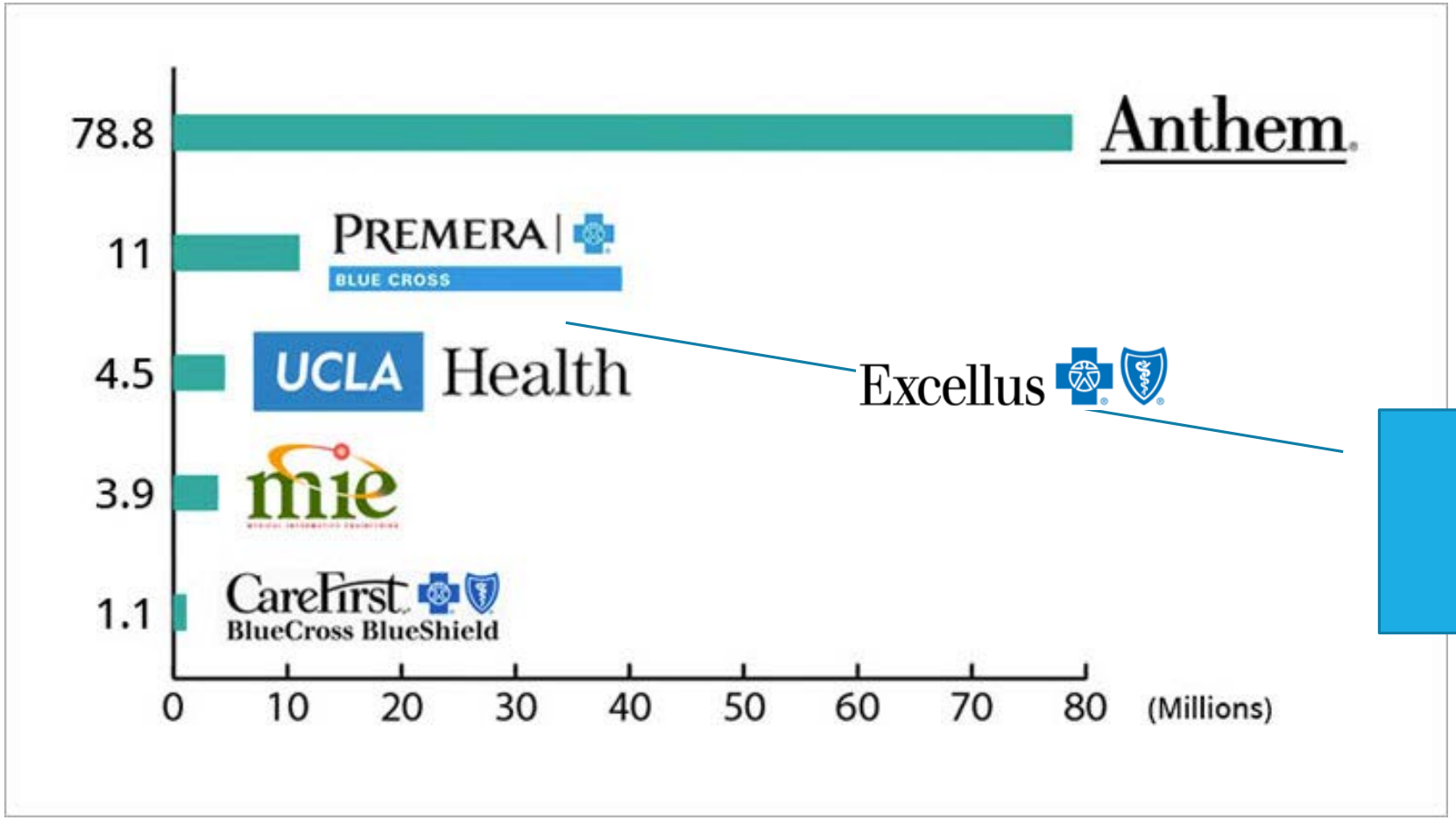
(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual……

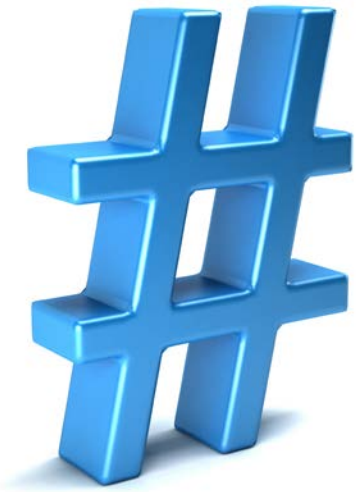
……. the entity must take such steps as are **reasonable in the circumstances** to destroy the information or to ensure that the information is de-identified.

Healthcare Data Breaches
Over 100 Million Affected in 2015



Excellus = additional 10,000,000

topics



- **legislative patchwork**

  (introduction to Australian legal framework on health information protection)

- **what is ‘reasonable’**

  (privacy demands ‘reasonable security’ and confidentiality measures – what does that entail in today’s cyber world)?

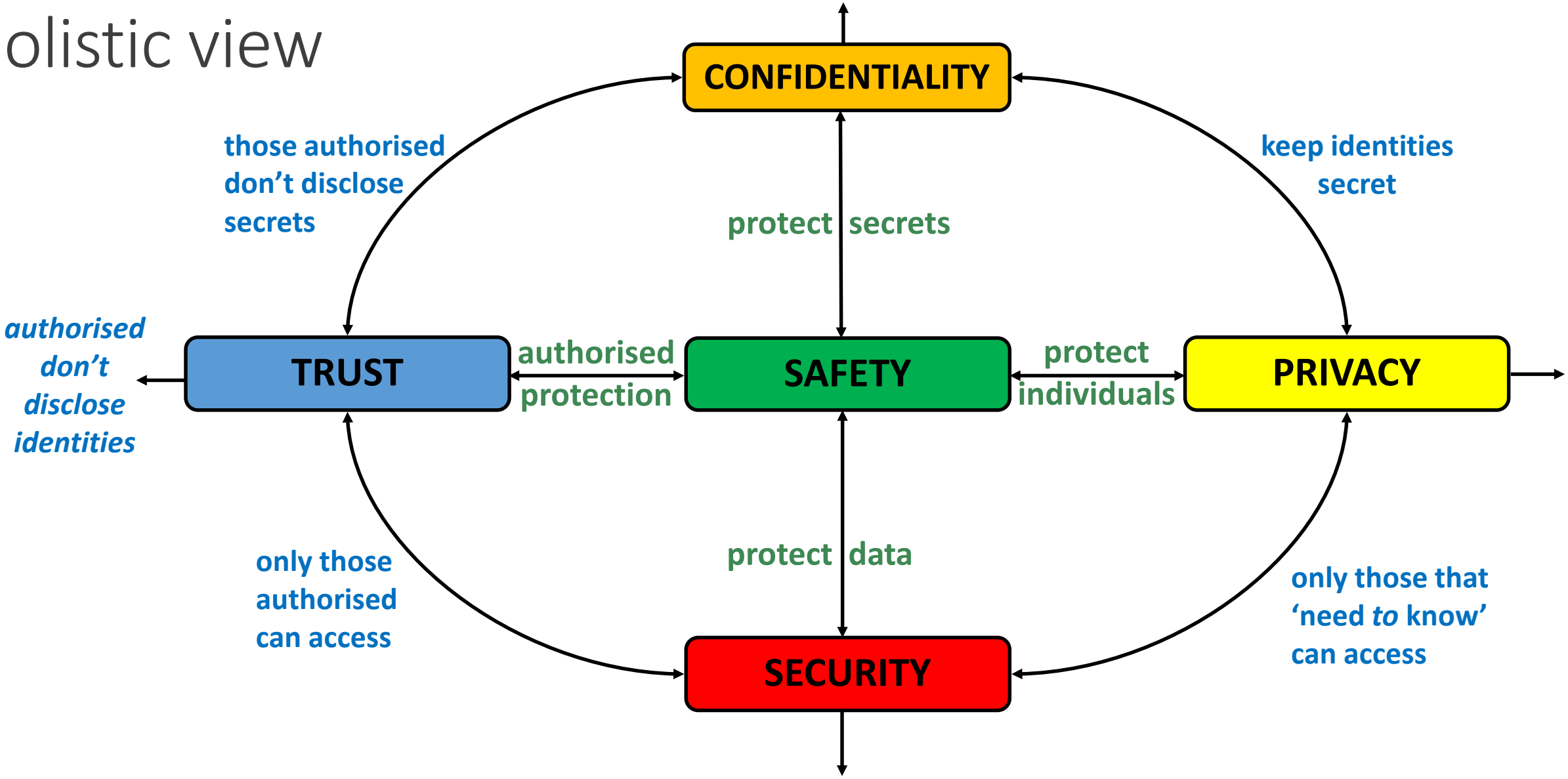
- **holistic approach**

  (the necessity to take a holistic view on to minimise privacy risks to acceptable levels)

Holistic approach

- protection needs to be much broader than **security**
- protection of patient **privacy** and **confidentiality**
- **trust** determines our willingness to participate
- the most important considerations is **safety**
- a system is considered safe, when the risk of harm is at an acceptable level
- you can avoid risks, accept risks, transfer risks or reduce risks
- risk of harm to individuals, business, environment and the IT systems itself
- resulting from breaches and other undesirable events with negative impacts

holistic view



Top 10 Questions regarding the Protection of Information

Q#	Chart Label	Related Question	Examples
1	‘protect individuals’	Are the measure in place adequate to minimise harm that could result from identifying individuals and disclosing their personal information?	Highly sensitive information may need extra care to ensure the individual it belongs to is not harmed though disclosure. HIV status is one such example that can have significant negative consequence for an individual such as their employment.
2	‘protect data’	Are the security measure adequate to protect unauthorised access?	For example, taking reasonable security measures, such as encryption, when using cloud services to store personal or confidential information.
3	‘protect secrets’	Have any company secrets or personal information been adequately classified for protection?	To protect against harm it is necessary to ensure the safety of information matches the confidentiality levels. For example, if the home address or movements of personnel is not classified as ‘confidential’ then this could but staff in danger; whereas if government secrets are not appropriately classified then this could cause serious or even exceptionally grave damage if this was to fall into the wrong hands.
4	‘authorised protection’	Can you trust those who are authorised with information protection?	The staff authorised to protect safety (i.e. protect individuals, the system and the environment) have been vetted and suitably trained? For example, using unqualified staff who have not been subject to police checks puts a higher risk on system safety.
5	‘only those that ‘need to know’ can access’	Are the measure in place adequate for limiting access to secrets and personal information to only those personnel that ‘need to know’?	For example, authorised users that can access personal information that is not part of their case load. If suitable role-based access control cannot be practically implemented, then does the company have any audit trails implemented that can check whenever inappropriate access has occurred?
6	‘restrict access to secrets’	Are the measure in place adequate for limiting access to secrets and personal information based on classification levels?	The company’s confidentiality levels are not suitably matched by the security measured put in place. For example, any ‘top secret’ documents that are not encrypted and are accessible without using two factor authentication.
7	‘only those authorised can access’	Are the measure in place adequate to limit access to only those appropriately authorised?	A common habit of sharing passwords or leaving the terminal unlocked can permit unauthorised access. It may also be necessary to validate users and checking their credentials. For example, achieving this via a phone call is not safe and a common method of social engineering used by adversaries.
8	‘authorised don’t disclose identities’	Are the measure in place adequate to ensure those authorised don’t disclose the identities of individuals?	Staff who have had suitable privacy training will ensure they verify who they are dealing with and what it is appropriate to disclose and to whom. For example, poor practices such as asking somebody if they are the Mr Lee who lives at Union Road could be disclosing information to close family members.
9	‘those authorised don’t disclose secrets’	Are the measure in place adequate to ensure those authorised don’t disclose secrets or personal information?	Authorised staff can permit breaches of confidentiality through poor practices such as not suitably identifying, labelling and handling confidential information. For example, use of shared drives for the convenience of file transfers with confidential information.
10	‘keep identities secret’	Do the confidentiality measure in place ensure that identity of individuals are not inappropriately disclosed?	The use of individual’s real names on accounts or equivalent labels could disclose which individuals are using the system. This could be critical if, for example, the accounts related to confidential services such as healthcare.

Video that explains all this is at:

www.PeterCroll.com

In conclusion

- When protecting sensitive information, the core attribute needs to be **Safety**
- **Privacy**, **Security**, **Confidentiality** and **Trust** should be mapped against **Safety** and each other.
- This will generate 10 key questions from which other critical questions can be derived
- For a system to be regarded as safe, risks must be managed to acceptable levels
- By **avoiding** the risk within your system, **accepting** them, **transferring** to a third party or **reducing** the risk e.g. improved protection mechanisms
- Risk analysis, requires knowledge of the **IMPACTS** that can result from undesirable events, such as a privacy breach.

In conclusion

- Generating a hierarchical listing of harm (individuals, systems and the environment) ensure a comprehensive analysis of negative impacts
- Risk analysis also requires estimates of the **LIKELIHOOD** of an undesirable event occurring
- Having appropriately analysed and managed the risks, will ensure you have the knowledge to develop a safe system that protects sensitive information
- The **holistic** approach, ensures you have covered both the **technical** and **human** issues that can put the safety of your systems at unnecessary risk.
- Not taking a holistic view, will leave your system vulnerable, and asking the question – **WHAT DID I MISS?**

Thank You