CYBER LAW

Your responsibilities to the law, patients and partners

Melissa Tan, Partner, Lander & Rogers

23 July 2023

KEY CONTACT

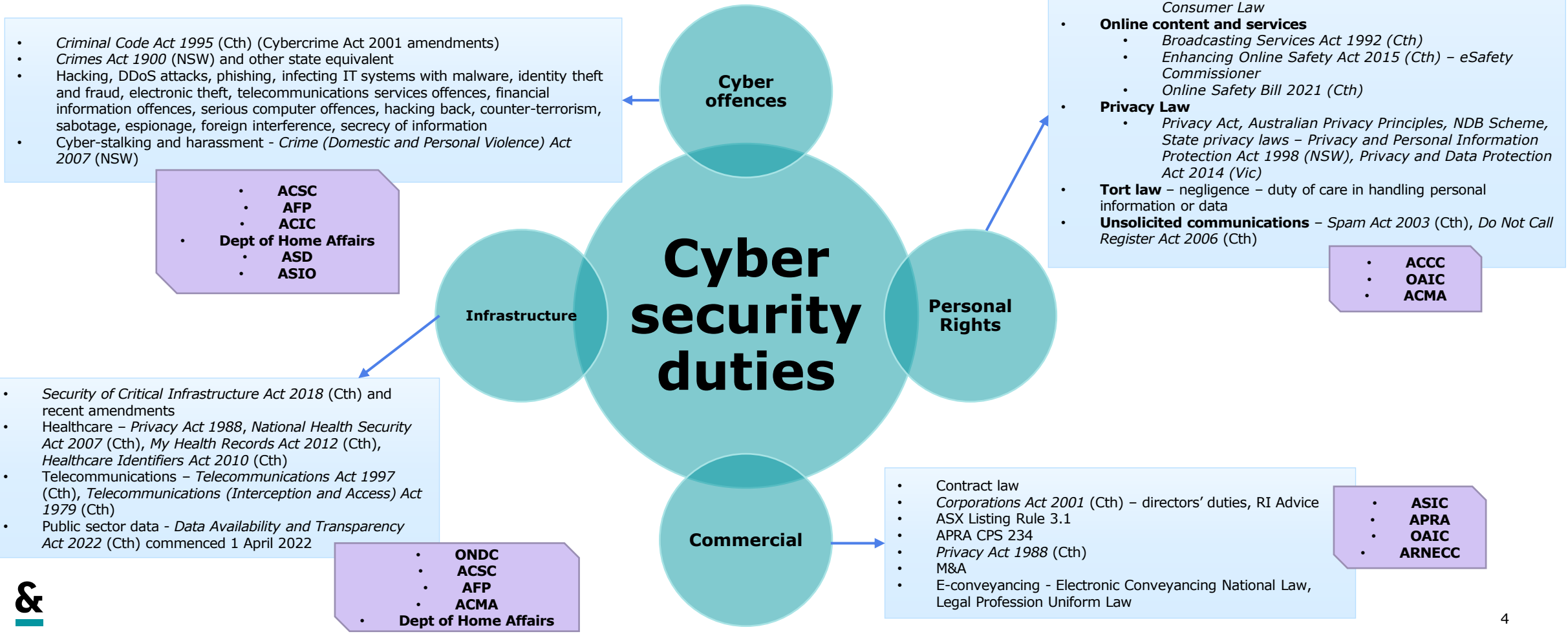
Melissa Tan
Partner and Head of Cyber Insurance

D +61 2 8020 7889
M +61 0438 742 770
E mtan@landers.com.au

WHAT IS CYBER LAW?

THE EVOLVING DUTIES LANDSCAPE

SOURCES OF CYBER SECURITY DUTIES AND OBLIGATIONS



A TALE OF WILMINGTON SURGICAL ASSOCIATES…

Wilmington Surgical Associates Facing Class Action Lawsuit Over Netwalker Ransomware Attack

Posted By Steve Alder on Feb 19, 2021

A TALE OF WILMINGTON SURGICAL ASSOCIATES

Wilmington Surgical Associates
General and abdominal surgery, breast surgery, oncologic surgery, and bariatric surgery

Netwalker Ransomware attack on WSA
Data Breach – two servers 13 GB of data

19 October 2020

Data leaked
Practice's financial information, employee information, patient data – photos, scanned docs, lab test results, Social Security numbers, health insurance information, other sensitive information

Class Action
Jewett et al. v. Wilmington Surgical Associates

10 February 2021

28 July 2020

FBI Flash Warning on Netwalker Ransomware

17 December 2020

Notifications
Affected individuals (115,000) and DHHS

Allegations

Failed to adequately monitor its systems for network intrusions. "The data breach was a direct result of defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect [personally identifiable information] and [protected health information] of its patients"

Negligent for failing to adequately safeguard patient data when it had been **put on notice (FBI warning) about the elevated risk** of ransomware attacks

Employees **failed to properly monitor** the medical practice's computer network

Maintained personal medical information "in a reckless and negligent" manner

Failed to provide timely breach notifications to patients and adequate information on the types of information compromised in the attack

The plaintiffs seek reimbursement of out-of-pocket expenses, compensation for time spent dealing with the aftereffects of the breach, restitution, injunctive relief, seven years of credit monitoring services for breach victims, and for WSA to undergo policy changes with how it handles patient data, to improve data security and undergo annual security audits.

A FEW LESSONS...

What does the WSA case highlight?

1. Your **cyber security risks**:

   Your practice is a valuable target!
   Sensitive Health Data = $

2. Your **legal obligations**

3. **Legal and other implications** of a cyber attack for your practice

YOUR CYBER SECURITY RISKS…

WHO ARE THE THREATS?

External

- *Threat actors / cyber criminals / Ransomware gangs*
- *Vulnerable suppliers or partners with access to your data or systems*

Internal

- *Yourself*
- *Employees – insider threat*

WHAT IS AT RISK?

More than data…

Data Privacy

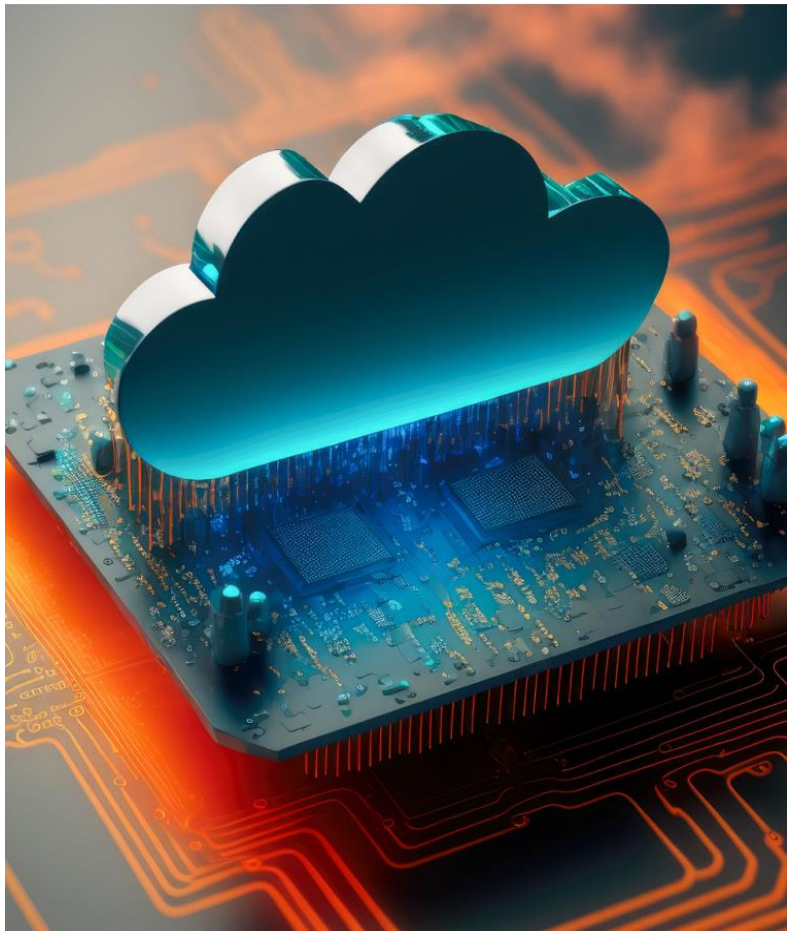
- Personal and sensitive information of patients such as photographs, Medicare details, lab test results and medical records
- Employee personal information (including information outside of employee records exemption such as TFN)
- Payroll, credit card

Patient Health

- Medical devices
- Medical equipment
- Systems used for diagnosis, monitoring and treatment

Surgery Practice's / Hospital's Operations

- Staff rotation and scheduling database
- Administration
- Practice management
- Appointment booking systems
- Inventory systems



HEALTHCARE IS AN ATTRACTIVE TARGET

Why is the healthcare sector such a valuable target for cybercriminals?

Healthcare data and research data valuable

- Cybercriminals are motivated by profit. Health records and other patient-related sensitive information are high-value trade items on the dark web

Healthcare staff unprepared / Education

- Healthcare staff work long hours under constant pressure. With the additional pressures on the healthcare system due to the pandemic, healthcare staff are often not alive to the possible cyber threats. **Human error** increases

Legacy technology

- Many healthcare providers continue to use outdated and unsupported software and operating systems

Multiple entry points and broad attack surface

- The adoption of more internet-connected devices in recent years has opened up a larger attack surface in the healthcare sector
- The Internet of Things (IoT) medical ecosystem

MULTIPLE VULNERABLE POINTS

1. Networks

- Without tight access control, once hackers breach a point in the hospital / clinic network, they can move freely within and laterally to access other critical assets

2 Internet of Things (IoT)

- Connected medical devices often lack built-in security features

3. Personal Devices

- Doctors and nurses add to vulnerabilities by connecting their personal devices to the hospital /clinic network or share patient details

4. Data Storage

- Storing electronic medical records, payment and insurance details in a single place increases potential damage from ransomware attackers

5. Records Disposal

- Privacy can be compromised by improper disposal of sensitive information

6. Your suppliers – supply-chain risk

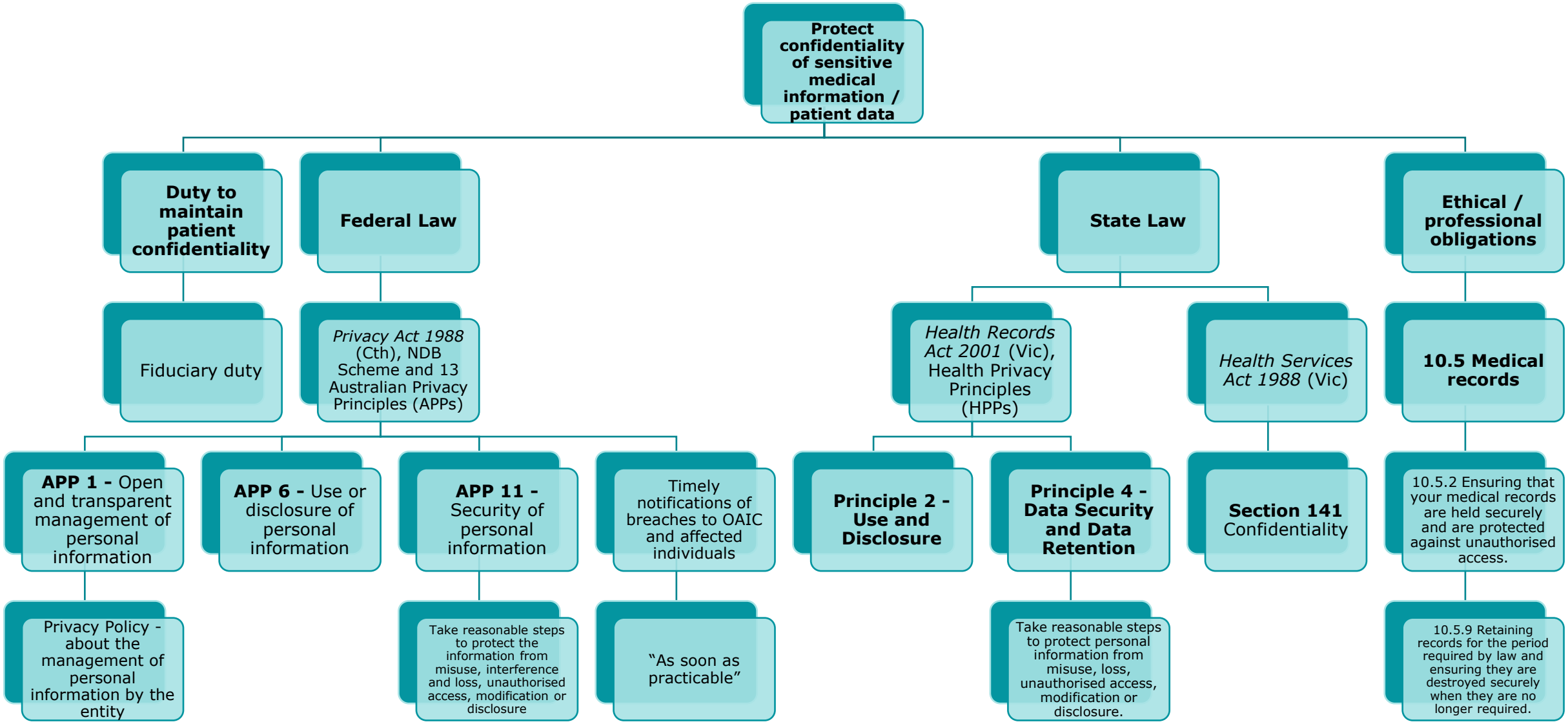
- If your partner or supplier with access to your systems is hacked and services taken offline, it may mean your patients' data is impacted and/or cause business interruption

https://www.wsj.com/articles/hospitals-suffer-new-wave-of-hacking-attempts-11612261802?mod=tech_lead_pos13

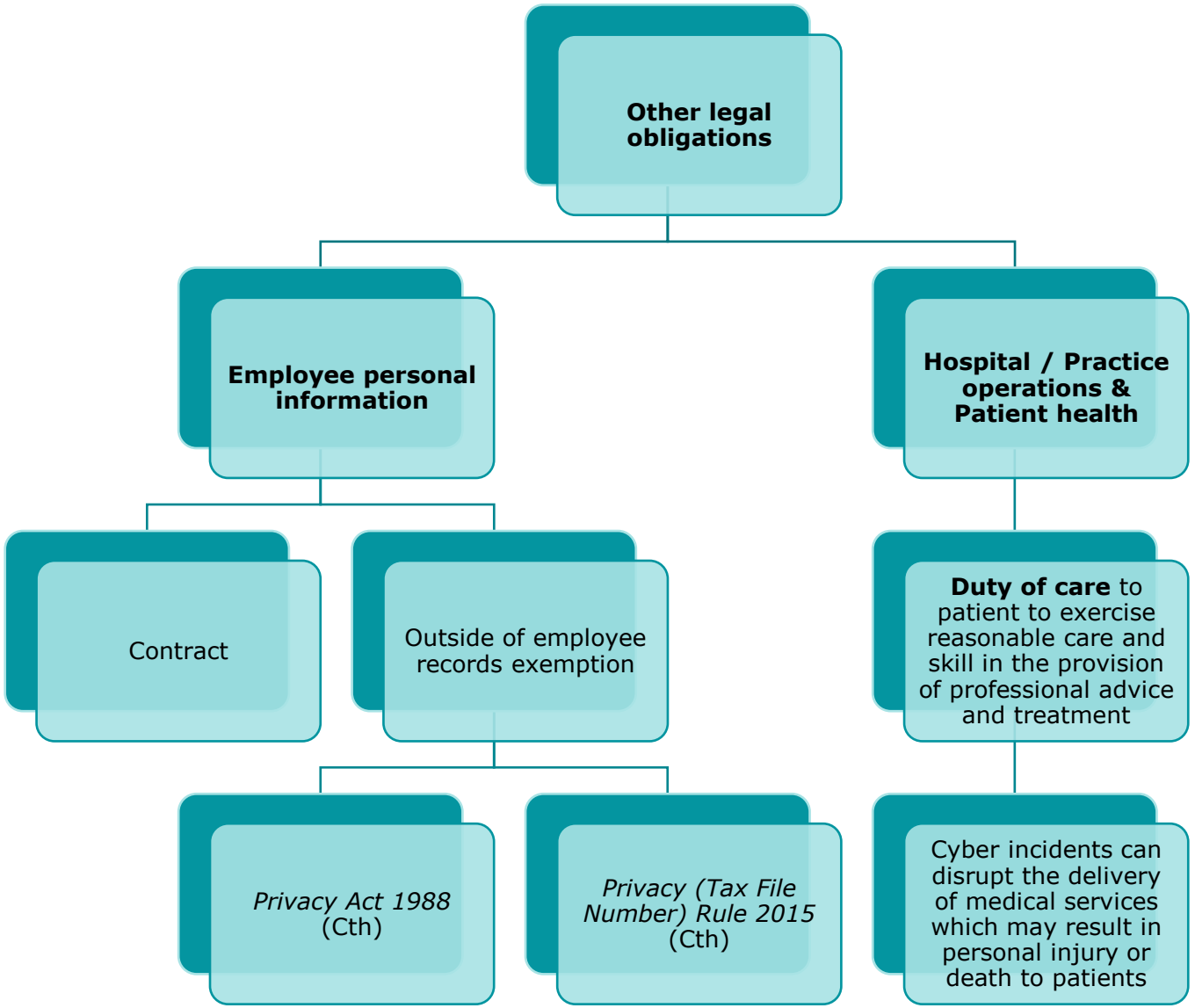
Diagram taken from Wall Street Journal article

YOUR LEGAL OBLIGATIONS…

YOUR LEGAL OBLIGATIONS – HEALTH INFORMATION

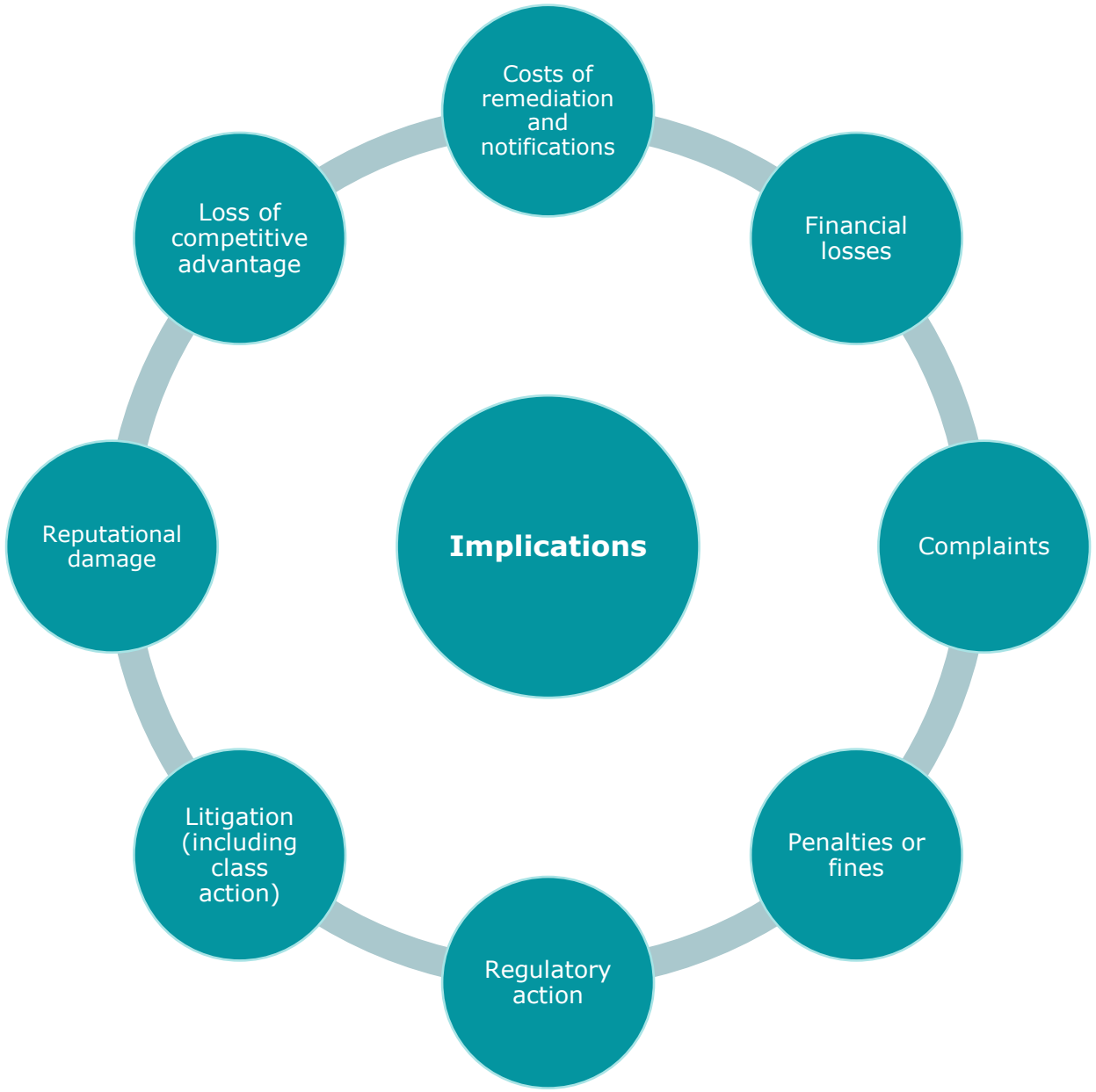


YOUR LEGAL OBLIGATIONS



LEGAL AND OTHER IMPLICATIONS

IMPLICATIONS OF CYBER INCIDENTS / DATA BREACHES



WHAT CAN YOU DO TO BE PREPARED?

HOW TO BE PREPARED?

KEY TAKEAWAYS

1. Health information is valuable

- They cannot be changed
- Risk of harm

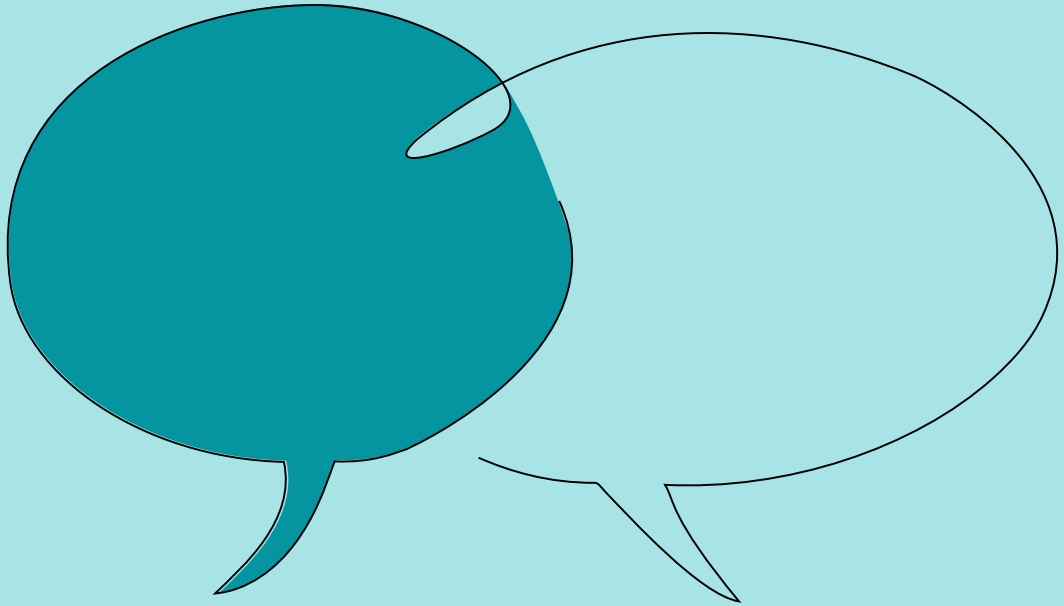
2. Protection of health information is key

- You have legal, ethical and professional obligations to protect the information from misuse, interference and loss, unauthorised access, modification or disclosure
- Relationship of trust

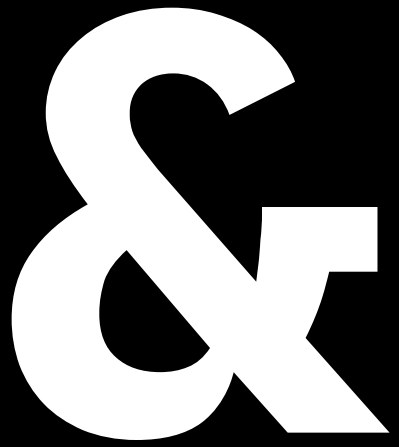
3. Human factor is key

- Minimise human error
- Make the human factor your strongest defence

QUESTIONS



THANK YOU



This presentation cannot be regarded as legal advice. Although all care has been taken in preparing this presentation, readers must not alter their position or refrain from doing so in reliance on this presentation. In particular, the clauses included in this presentation are randomly selected from sample project documents and are not to be assumed to be drafting models. Where necessary, advice must be sought from competent legal practitioners. The author does not accept or undertake any duty of care relating to any part of this presentation.

Melbourne

T +61 3 9269 9000
F +61 3 9269 9001

Sydney

T +61 2 8020 7700
F +61 2 8020 7701

Brisbane

T +61 7 3456 5000
F +61 7 3456 5001