IT & Privacy Laws

(for Aged Care providers)

Presented by:

Alison Choy Flannigan
Partner – Health, aged are & life sciences
(02) 9390 8338
alison.choyflannigan@holmanwebb.com.au

HOLMANWEBB LAWYERS

Introduction

- **Privacy**
  - What is privacy?
  - Privacy laws
  - Australian Privacy Principles The Personally Controlled Electronic Health Record
  - Social media
  - Relevant privacy cases

HOLMANWEBB LAWYERS

Privacy

- **Why is privacy important?**
- Information collected in providing community, health and aged care services is more than just data and statistics.
- It often reflects a person's:
  - Medical condition (including HIV status)
  - Mental health
  - Lifestyle
  - Sexual preference
  - Personal history (in terms of sexual or other abuse)
  - Family history
  - Beliefs
- *You are a custodian of a person's secrets*
- *Misuse of health information has led to patient suicide….*

- *We need to be culturally sensitive to personal information, for example, in relation to the indigenous population*

HOLMANWEBB LAWYERS

Privacy

- **To whom does the Commonwealth legislation apply?**
  - Commonwealth government agencies and private sector
  - Whilst there are is a small business operator exemption (annual turnover of $3 million or less for a financial year) – this does *not* apply to health information except in an employee record
  - The APPs extend to an act done or practice engaged in and outside Australia by an organisation that has an "Australian link"
    - Australian company
    - Someone who carries on business in Australia
    - Information is collected or held in Australia
    - Websites which offers goods and services in Australia
    - Australia is a country in a drop down menu on the entity's website
  - State laws apply to State government agencies
  - The Cth Privacy Act applies to medical practitioners in their right of private practice

HOLMANWEBB LAWYERS

Privacy

- **Privacy Legislation (private sector)**
  - *Privacy Act 1988 (Commonwealth) – penalties for serious and repeated offences are up to $1.7 million for businesses and $340,000 for individuals*
  - *Health Records and Information Privacy Act 2002 (NSW)*
  - *Health Records Act 2001 (Vic)*
  - *Health Records (Privacy and Access) Act 1997 (ACT)*

Note: The Australian Law Reform Commission Report "*For your Information: Australian Privacy Law and Practice*" (ALRC 108)

HOLMANWEBB LAWYERS

Privacy

- **Special rules for health records**

- Health information is “sensitive information”
- Use and disclosure is permitted if there is a serious and imminent threat to the health and safety of an individual or the public
- Use and disclosure for health and medical research if certain conditions are met eg NHMRC guidelines
- Disclosures to carers for compassionate reasons
- Restrictions on access if providing direct access would pose a serious threat to the life or health of any individual
- Use and disclosure of genetic information to lessen or prevent a serious threat to a genetic relative
- The collection of family, social and medical histories is permitted in some circumstances – Public Interest Determination No 12A

HOLMANWEBB LAWYERS

Privacy

- **Key concepts**
  - **“personal information”** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

HOLMANWEBB LAWYERS

Privacy

- **Key concepts**
  - **"health information"** means:

(a) information or an opinion about:

(i) the health or disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body part, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual

Privacy

- **Key concepts**
  - **"health service"** means:
    (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
      (i) to access, record, maintain or improve the individual's health; or
      (ii) to diagnose the individual's illness or disability; or
      (iii) to treat the individual's illness or disability or suspected illness or disability; or
    (b) the dispensing on prescription of a drug or medical preparation by a pharmacist

Privacy

- **Australian Privacy Principles (Privacy Act)**
  - APP 1 Open and transparent management of personal information
  - APP 2 Anonymity and pseudonymity
  - APP 3 Collection of solicited personal information
  - APP 4 Dealing with unsolicited personal information
  - APP 5 Notification of the collection of personal information
  - APP 6 Use of disclosure of personal information
  - APP 7 Direct marketing
  - APP 8 Cross-border disclosure of personal information
  - APP 9 Adoption, use and disclosure of government related identifiers
  - APP 10 Quality of personal information
  - APP 11 Security of personal information
  - APP 12 Access to personal information
  - APP 13 Correction of personal information

Privacy

- **Australian Privacy Principles (Privacy Act)**
  - **APP 8 Cross-border disclosure of personal information**

Before an you disclosespersonal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

You must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

HOLMANWEBB LAWYERS

Privacy

- **Australian Privacy Principles (Privacy Act)**
  - Subclause 8.1 does not apply to the disclosure of personal information to an overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

Privacy

- **Australian Privacy Principles (Privacy Act)**
  - Subclause 8.1 does not apply to the disclosure of personal information to an overseas recipient if:

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Privacy

- **Australian Privacy Principles (Privacy Act)**
  - **APP 11 Security of personal information**

    - You must take such steps as are reasonable in the circumstances to protect the information:
      - from misuse, interference and loss; and
      - from unauthorised access, modification and disclosure
    - If you no longer need the personal information for any purposes which the information may be used or disclosed and the information is not contained in a Commonwealth record or required to be law or a court/tribunal order to be retained, you must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified

HOLMANWEBB LAWYERS

Privacy

- **Privacy Cases**
  - **Australian - Pound Road Medical Centre (July 2014)**

HOLMANWEBB LAWYERS

Privacy

- **Privacy Cases**
  - **USA - Parkview Health System (June 2014) $800,000 HIPAA settlement**

HOLMANWEBB LAWYERS

Privacy

- **Privacy Cases**
  - **Cupid Media Pty Limited: Own motion investigation report [2014] AICmr CN 3 (25 June 2014)**
    - More stringent steps are required to keep sensitive information secure
    - Information and patch management systems
    - Testing and monitoring steps
    - Keep passwords encrypted using strategies such as hashing and salting
    - Take reasonable steps to destroy or permanently de-identify the personal information held in relation to accounts no longer in use or needed
    - Engaged a security team to conduct a full audit.
    - Develop and implement a data breach response plan
    - Daily hacking and vulnerability scans
    - Review best practice data storage methods
    - Conducted a review of personal information to ensure you are collecting and retaining personal information that is necessary
    - Procure and install additional firewall security hardware
    - De-identify personal information relating to old or inactive user accounts

Privacy

- **Personally controlled electronic health record**
  - The PCEHR is an electronic medical record sponsored by the Commonwealth Government – www.nehta.gov.au
  - Health care providers and consumers " opt-in"
  - It is not a full clinical record
  - The consumer controls the content and has their own section to enter information which is separate to the clinical section
  - Patients can remove documents but can not edit the record, other than consumer entered notes
- ***Personally Controlled Electronic Health Records Act 2012*** **(Cth)**
  - **Section 59** – Unauthorised collection, use and disclosure of health information included in a consumer's PCEHR which is not authorised under Division 2 and the person knows or is reckless as to that fact – 120 penalty units ($20,400) and x 5 for bodies corporate ($102,000).

Privacy

Don’t forget that your privacy obligations extend to social media!

HOLMANWEBB LAWYERS

Risk management

- **Privacy risks with IT**
  - Be mindful of your legislative obligations under privacy laws
  - Ensure that the information which is uploaded is accurate and up to date
  - Ensure that you have a privacy policy and keep it up to date
  - Data security issues
  - Develop a data breach response plan
  - Check consumer identity and verification
  - Ensure that appropriate arrangements are in place in relation to cross-border data flows
  - Destroy or permanently de-identify the personal information held which is no longer in use or needed
  - Provide training and education of your staff on privacy requirements

Conclusion and questions

alison.choyflannigan@holmanwebb.com.au

HOLMANWEBB LAWYERS