Australian Privacy Laws and Health Information

Author: Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia
October 2013

Australia privacy rights are regulated by Commonwealth and State legislation and the laws protecting confidential information under the common law.

Australian privacy laws govern the collection, use and disclosure of "personal information". Further, individuals are provided with a right of access and correction of their own personal information. There are also data security, data quality and cross-border transborder data flow requirements.

Under Australian privacy laws:

- "**personal information**" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an *individual whose identity is apparent*, or can reasonably be ascertained, from the information or opinion"

In Australia, health information (such as medical records) are a subset of personal information and attract additional protection and rules. These include:

- 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;
- 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.

"**health information**" means:

(a) information or an opinion about:

(i) the health or a 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 parts, 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.

- "**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 assess, 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 medicinal preparation by a pharmacist.

The *Privacy Act 1988 (Commonwealth)* (**Privacy Act**), which applies to Australian Commonwealth government agencies and private sector organisations, has been recently amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* (**Privacy Amendment Act**). The Privacy Amendment Act was passed by Parliament on 29 November 2012, received the Royal Assent on 12 December 2012 and comes into force on 12 March 2014.

The amendments aim to:

- create a single set of Australian Privacy Principles applying to both Australian Government agencies and the private sector. These principles will replace the existing Information Privacy Principles and National Privacy Principles;
- introduce more comprehensive credit reporting, improved privacy protections and more logical, consistent and simple language;
- strengthen the functions and powers of the Australian Information Commissioner to resolve complaints, use external dispute resolution services, conduct investigations and promote compliance-penalties of up to 2000 penalty units $340K for individuals – x 5 for body corporates AUD$1.7 million; and
- create new provisions on privacy codes and the credit reporting code, including codes that will be binding on specified agencies and organisations.

Australian Privacy Principles

The Privacy Amendment Act introduces a unified set of Australian Privacy Principles which apply to both Commonwealth agencies and the Australian private sector, replacing separate public and private sector principles.

Permitted health situations

The Privacy Amendment Act introduces the concept of "permitted health situation" in a new section 16B.

Collection – provision of a health service

A "permitted health situation" exists in relation to the collection by an organization of health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and
(b) either:

(i) the collection is required or authorised by or under an Australian law (other than the Privacy Act); or
(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

Collection – research etc.

A "permitted health situation" exists in relation to the collection by an organisation of health information about an individual if:
(a) the collection is necessary for any of the following purposes:
(i) research relevant to public health or public safety;
(ii) the compilation or analysis of statistics relevant to public health or public safety;
(iii) the management, funding or monitoring of a health service; and
(b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and
(c) it is impracticable for the organisation to obtain the individual's consent to the collection; and
(d) any of the following apply:
(i) the collection is required by or under an Australian law (other than the Privacy Act);
(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations
of professional confidentiality which bind the organisation;
(iii) the information is collected in accordance with guidelines approved under section 95A of the purposes of this subparagraph.

Use or disclosure – research, etc.

A "permitted health situation" exists in relation to the use or disclosure by an organisation of health information about an individual if:
(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the organisation to obtain the individual's consent to the use or disclosure; and
(c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes this paragraph; and
(d) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

Use of disclosure – genetic information

A "permitted health situation" exists in relation to the use or disclosure by an organisation of genetic information about an individual (the first individual) if:
(a) the organisation has obtained the information in the course of providing a health service to the first individual; and
(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and
(c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and
(d) in the case of disclosure – the recipient of the information is a genetic relative of the first individual.

Disclosure – responsible person for an individual

A "permitted health situation" exists in relation to the disclosure by an organisation of health information about an individual if:
(a) the organisation provides a health service to the individual; and
(b) the recipient of the information is a responsible person for the individual; and
(c) the individual:
  (i) is physically or legally incapable of giving consent to the disclosure; or
  (ii) physically cannot communicate consent to the disclosure; and
(d) another individual (the carer) providing the health service for the organisation is satisfied that either:
  (i) the disclosure is necessary to provide appropriate care or treatment to the individual; or
  (ii) the disclosure is made for compassionate reasons; and
(e) the disclosure is not contrary to any wish:
  (i) expressed by the individual before the individual became unable to give or communicate consent; and
  (ii) of which the care is aware, or of which the carer could reasonably be expected to be aware; and
(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan, Partner, Holman Webb
P: +61 2 9390 8338
E: alison.choyflannigan@holmanwebb.com.au

Update on Personally Controlled Electronic Health Records - Legal and Privacy Issues

Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia

October 2013

As part of the 2010/11 Federal budget, the Government announced a $466.7 million investment over two years for a national Personally Controlled Electronic Health Record (**PCEHR**) system for all Australians who choose to register on-line, from 2012-2013. This initiative has the potential to be a revolutionary step for Australian health care, in terms of both consumer's access to their own health information and improvement in information which will be available to health professionals when they treat a patient.

To date, the uptake has been slow. NeHTA scorecard as at July 2013

- The total number of people who registered for an eHealth record as at May 31 2013 was 612,391.
- More than 4,502 healthcare provider organisations have signed onto the eHealth Record system.
- 6567 individual doctors, nurses and other healthcare providers throughout Australia has been authorized by their organisations to access the PCEHR system;
- More than 15.25 million documents have been uploaded into the PCEHR system.

Aims of PCEHR include:

- Reduce risks in the health system;
- Fewer patients will experience adverse events
- Improve access to health records and thereby reduce medication errors.

Some key concepts are:

• Individuals are able to choose whether or not to have a PCEHR and will be able to set their own access controls and may withdraw at any time.
• The PCEHR will contain clinical documents such as Shared Health Summaries, Discharge Summaries, Event Summaries, Pathology Result Reports, Imaging Reports and Specialist Letters. It may also include key health information entered by the individual such as over-the-counter medicines and allergies and access information

from Medicare Australia such as an individual's organ donor status, dispensed medications funded under the PBS, information about healthcare events from an individual's Medicare claiming history and a child's immunisation history. The PCEHR may also contain an individual's advance care directives (if any). The PCEHR is, however, not a comprehensive health record.

• Healthcare organisations can choose to participate and will need a healthcare organisation identifier (HPI-O). They must agree to use appropriate authentication mechanisms to access the PCEHR and use software that has been conformance tested to be used with the PCEHR system.

• Health information within the PCEHR system is protected through a combination of legislation, governance arrangements and security and technology measures, including under the *Personally Controlled Electronic Health Records Act 2012 (Cth).*

The PCEHR legislation imposes penalties for intentional or reckless unauthorized collection, use and disclosure of health information; Fines up to 120 penalty units for individuals (AUD$20,400); and x 5 penalties for bodies corporate AUD$102,000. One Commonwealth penalty unit is currently AUD$170.

There are a number of medico-legal and privacy issues which arise with the PCEHR. Some of these are summarised below:

Medico-legal

• If a medical practitioner consults with a patient and is negligent in entering information onto the PCEHR, there are more clinicians relying upon it, so the potential for liability from a negligent assessment of a patient or negligently prepared medical record increases.

• Health professionals must be mindful that the PCEHR is not a complete medical record and must continue to be vigilant in continuing to obtain independent information from patients. Information may be excluded from the PCEHR at the request of a patient and missing information is unlikely to be flagged.

• If a medical practitioner has relied upon information on the PCEHR which is incorrect, then the medical practitioner will need to track the author of the original information to join as a cross-defendant.

• If a patient instructs a medical practitioner not to include information on the PCEHR then the medical practitioner will be under an obligation to inform the patient the risks and consequences of this.

• Direct access to a medical record may be denied if providing access would pose a serious threat to the life or health of any individual. In those cases, the patient is usually provided access through another medical practitioner. If consumer access requests are dealt with centrally, measures should be implemented to ensure that a clinical assessment is made in relation to whether or not a patient's request for access or information could pose a serious threat to the life or health of any individual. Arguably such information should not be included in the PCEHR.

• Often a request for access can be an indicator of a potential claim which can be resolved quickly by the clinician by early discussions with the patients. There should be a mechanism so that relevant clinicians are informed if there is a potential claim early.

Privacy issues

There are also a number of privacy issues, including:

• Obtaining adequate privacy consent from patients;
• Ensuring that the systems can accurately implement the consent options of patients, such as limiting access or prohibiting access to the PCEHR to health professionals nominated by patients.
• Ensuring that only information which is required to provide treatment for the patient is collected.
• Privacy issues if the system involves a number of system vendors and subcontractors or cloud computing.
• Uniformity of the usage of medical terms and abbreviations and clear handwriting is preferred to protect data quality.
• Clear understanding of the information flows and potential for leakage of personal health information to unapproved persons or overseas.
• Data security issues.
• Patient and participating health professional identification and verification issues.
• Education and training of participating health professionals.

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan
Partner, Holman Webb
T: +61 2 9390 8338
E: alison.choyflannigan@holmanwebb.com.au

This article is provided for general information purposes only and should not be relied upon as legal advice.

Mobile Medical Apps – When are they medical devices?

Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia

October 2013

Like the US, Australia is experiencing the proliferation of mobile medical apps (software applications that can be executed on a mobile platform) which seek to provide a number of functionalities, many of which operate between traditional disease management and health and wellness. Some of these new apps assist consumers with their health and wellness management, whilst others provide healthcare providers with tools to improve and facilitate the delivery of patient care.

United States

The US Food and Drug Administration (FDA) released the *Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff* on 25 September 25 2013.

The US Guidance explains how the FDA intends to regulate select software applications intended for use on mobile platforms.

The FDA defines a "**mobile medical app**" as a mobile app that meets the definition of "device" in section 201(h) of the *Federal Food, Drug, and Cosmetic Act* (**FD&C Act**) and includes an application that:

• is used as an accessory to regulated medical device, for example a remote display to a medical monitor; or

• transforms a mobile platform into a regulated medical device, for example an attachment to a blood glucose strip.

The intended use of the mobile app determines whether it meets the definition of a "device". As stated in 21 CPR 801.4, intended use may be shown by labelling, claims, advertising materials, or oral or written statements by manufacturers or their representatives. When the intended use of a mobile app is for the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of man, the mobile app is a device.

The FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were not to function as intended.

Mobile medical apps that meet the definition of a device must follow the regulation required for the particular class of device classification.

The FDA will apply regulatory oversight in respect of applications which allow the user to input patient-specific information and, using patient-specific formulae or algorithms, output a patient-specific result, diagnosis or treatment recommendation to be used in clinical practice or to aid in making clinical decisions.

There are three categories:

1. Mobile apps which are **not** medical devices;
2. Mobile medical apps which *may* be medical devices and for which the FDA intends to exercise ***enforcement discretion*** (meaning that the DFA does not intend to enforce requirements under the FD& C Act; and
3. Mobile medical apps which are the focus of FDA's regulatory oversight (mobile medical apps);

The US Guidance does **not** consider the following as medical apps:

- mobile apps containing only medical reference materials or educational tools for medical training, which do not contain patient specific information;
- mobile apps that are intended for general patient education and facilitate patient access to commonly used reference information, treatment, or prevention of a disease;
- mobile apps that automate general office operations in a healthcare setting and are not intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation;
- medical apps which are generic aids, for example a magnifying glass; and
- mobile apps that perform the functionality of an electronic health record system.

Examples of mobile apps which ***may*** meet the definition of medical devices but which the FDA intends to exercise ***enforcement discretion*** because they pose lower risk to the public include:

- mobile apps that help patients with diagnosed psychiatric conditions by providing a "skill of the day" behavioral technique or messages which can be accessed to decrease anxiety;
- mobile apps that us GPS location information to alert asthmatics of environmental conditions;
- mobile apps which use video and video games to motive patients to do their physical therapy exercises at home; and
- mobile apps which advise on interactions between herbs and drugs.

The following are examples of **regulated mobile apps**:

- mobile apps that transform a mobile platform into a regulated medical device, such as mobile apps which use a sensor or electrode to measure blood oxygen saturation;
- mobile apps that connect to an existing device type for the purposes of controlling its operation, function or energy source, for example, a mobile app which controls an infusion pump or a cochlear implant;
- mobile apps that display, transfer, store or convert patient-specific medical device data from a connected device, for example, a device which connects to a nursing central station and displays medical data to a physician's mobile phone.

Manufacturers of mobile medical devices are subject to the requirements described in the applicable device classification regulations.

Australia

The Australian Therapeutic Goods Administration (TGA) regulates the quality, safety and performance of medical devices and uses a regulatory framework that includes software for therapeutic purposes which falls under the definition of a "therapeutic good" under the *Therapeutic Goods Act 1989 (Cth)*(**Act**).

In Australia, whether or not a mobile health and medical app is a "medical device" and "therapeutic good" (and regulated as such) depends principally upon:

1. functionality; and

2. the claims made in relation to the product

Therapeutic goods includes goods that are represented in any way to be, or that are, whether because of the way in which the goods are presented or for any other reason, likely to be taken to be for "therapeutic use" (as defined) and includes medical devices, subject to stated exceptions.

Section 41BD of the Act states that

A medical device includes:

(a) any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following:

i. diagnosis, prevention, monitoring, treatment or alleviation of disease;

ii. diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability;

iii. investigation, replacement or modification of the anatomy or of a physiological process;

iv. control of conception; and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means; or

b. an accessory to an instrument, apparatus, appliance, material or other article covered

by paragraph (a).

The Medical Technology Association of Australia (MTAA) in its submission on Apps Purchases by Australian Consumers on Mobile and Handheld Devices dated January 2013 recommended the "regulation of smartphone medical apps that are intended by the developer to cure, treat, monitor or diagnose a medical condition."

In that paper the MTAA mentions that the TGA has stated that it will regulate health apps for smartphones as the need arises.

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan, Partner

Holman Webb, Lawyers

Health, aged care & life sciences

E:alison.choyflannigan@holmanwebb.com.au

P: +61 2 9390 8338