Holman Webb
Lawyers

Privacy Update

March 2014

Contents

Introduction

Privacy Update

Privacy is an important and developing area of relevance to government, business and individuals.

If your business collects, uses or discloses personal information, maintains a client or customer database or uses a cloud computer system, changes to the laws commencing in March 2014 are relevant to you. Ignore them at your peril because the penalties for breaches are being significantly increased up to $1,700,000 for businesses and $340,000 for individuals.

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* includes a set of harmonised privacy principles that regulate the handling of personal information by both Australian Commonwealth government agencies and private sector businesses. These new principles are called the Australian Privacy Principles (APPs). They will replace the existing Information Privacy Principles (IPPs) that currently apply to Australian Government agencies and the National Privacy Principles (NPPs) that currently apply to private sector businesses.

Under the changes, there are 13 new APPs. A number of the APPs are significantly different from the existing principles, including APP 7 on the use and disclosure of personal information for direct marketing and APP 8 on cross-border disclosure of personal information.

For further information please contact any of the Partners listed on the last page of this update.

Privacy Law Reform in Australia – Overseas Recipients and the Cloud

Jonathan Casson, Partner

On 12 March 2014 significant changes to the Australian Privacy Act (Act) commenced, providing enhanced powers for the Australian Information Commissioner and changes to credit reporting laws. Australian privacy law tends to be thought of at the Federal level but each state and territory also has their own data protection legislation. The Office of the Privacy Commissioner is the Federal authority (www.oaic.gov.au.).

The Act applies to both the public and private sector (in respect of companies with a turnover greater than $AUD3,000,000 per year) and though currently separate privacy principles apply to the public sector and the private sector, the March 2014 reforms harmonise these principles into what will become known as the Australian Privacy Principles (APPs). These replace the existing Information Privacy Principles that apply to the public sector and the National Privacy Principles that apply to businesses.

Any business subject to the Act that collects, uses or discloses personal information, maintains a client or customer database or uses a cloud computer system, will be affected by the changes. Penalties for breaches are being significantly increased up to $1,700,000 for businesses and $340,000 for individuals.

Under the changes, there are 13 new APPs. A number of the APPs are significantly different from the existing principles, including APP 7 on the use and disclosure of personal information for direct marketing (see elsewhere in this Update) and APP 8 on cross-border disclosure of personal information.

The privacy laws protect Personal Information and Sensitive Information. Personal information includes information or an opinion about a person whose identity is apparent or can be reasonably ascertained from that information. The truth of the information is irrelevant. Sensitive Information relates to an individual's race or ethnic origin; political opinion; memberships of a political association; religious beliefs; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; and criminal record. Particular reference is made to health information and genetic information.

The amendments impose greater obligations on entities who disclose personal information about an individual to an "overseas recipient". Entities must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information (subject to specified exceptions noted below). The party that discloses the personal information to the overseas entity will be liable under Australian privacy law for breaches of the APPs committed by the overseas entity. Where a business sends personal information (including health information) to organisations overseas (for example for reporting of tests, records management or marketing), it must ensure that exemptions apply or the person from whom that information is collected is expressly aware of and consents to this. More detailed information will also need to be included in a business' corporate privacy policy.

Simply putting information on an overseas server is not disclosure (the Act calls this use). It becomes a disclosure only when the personal information is accessed by a third party. Accordingly, for example, providing personal information to a cloud service provider located overseas for the limited purpose of storage and access will be "use", not disclosure if the service contract so limits the use and the entity retains control over how the information is handled by the service provider.

The overseas disclosure of personal or sensitive information between related companies will be affected. The actions of the overseas entity might well impact upon the local subsidiary and put it at risk of fines or damages pursuant to a breach of the APPs. Accordingly, care must be taken to ensure that corporate privacy principles in multinational organisations, large and small, are designed to meet the requirements of Australian legislation where a breach might lead to loss. Generally, employment records are not caught up by the Act.

APP 8.1 provides that before an APP entity discloses personal 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;

the entity 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.

For example, the disclosing entity should adopt stringent contractual terms addressing data management, or otherwise not deal with the overseas recipient.

Furthermore, the prohibition on the disclosure of personal information about an individual to the overseas recipient does not apply if (in the case of businesses):

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 APP 8.1 will not apply; and

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

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 (which is described in a table) exists in relation to the disclosure of the information by the APP entity.

The explanatory memorandum that accompanied the Act's introduction noted that it is not intended to apply where information is merely routed through servers that might be outside Australia. Risk management procedures should be in place to prevent access to data in these cases.

Privacy Laws and Direct Marketing

Jonathan Casson, Partner and Louise Bavin, Lawyer

The Privacy Act has taken a new look at regulating direct marketing and deals with it specifically in APP7. APP7 is a new principle which has been carved out of what was formerly NPP2.

The privacy laws protect Personal Information and Sensitive Information. Personal information includes information or an opinion about a person whose identity is apparent or can be reasonably ascertained from that information. The truth of the information is irrelevant. Sensitive Information relates to an individual's race or ethnic origin; political opinion; memberships of a political association; religious beliefs; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; and criminal record. Particular reference is made to health information and genetic information.

Subject to what is said relating to non-sensitive information, in essence, organisations holding personal information must not use or disclose personal information for direct marketing unless:

- the information is collected directly from the individual; and
- the individual would reasonably expect the information to be disclosed for that purpose; and
- the organisation provides a simple means for the individual to easily request not to receive direct marketing communications; and the individual has not made such a request.

Non-sensitive information

In relation to the collection of non-sensitive information, if it is collected directly from an individual who would not reasonably expect it to be disclosed for direct marketing, or collected from a third party, then several requirements must be met. There must be consent or it must be impractical to seek consent. There must be a simple opt out mechanism and a prominent statement or notice to the effect in every direct marketing communication that the individual may refuse to receive any further material. Of course, if the individual opts out or makes such a request you must remove them from your direct marketing program.

Sensitive information

Sensitive information may be used or disclosed by an organisation for the purpose of direct marketing only if the individual has consented to use or disclosure for that purpose.

Commonwealth contractors

Further, a contracted service provider for a Commonwealth contract may use or disclose personal information for the purpose of direct marketing if this meets an obligation under the contract.

Non-Receipt Requests

Individuals may request not to receive direct marketing from the collecting organisation, and request the organisation not to use or disclose the information to facilitate direct marketing by other organisations. Individuals may also request the collecting organisation to provide its source of information.

Organisations must respond within a reasonable time period, without charge and, if requested, advise the source of information unless it is impracticable to do so.

Finally, APP7 does not overrule the *Do Not Call Register Act, 2006* and the *Spam Act, 2003*.

Privacy Act Reforms: Impact on Terms and Conditions of Trade and Credit Reporting

Jonathan Casson, Partner

The Privacy Act changes commenced this month. If your credit application, privacy policy or terms and conditions of trade do not property take the new amendments into account you may find yourself in danger of breaching the amended Act. The changes imposed new credit reporting provisions and adds enforcement powers to the privacy Commissioner. The new principles are called the Australian Privacy Principles intended to be harmonised across government and business. They replace the existing Information Privacy Principles that apply to government and the National Privacy Principles that currently apply to private sector business.

The changes are quite broad. The Privacy Commissioner, Timothy Pilgrim, suggests that businesses take a number of steps in the lead up to the new changes. He urges organisations to update their privacy policy. Compliance practices will need to respond to the changes. Clear systems and processes to handle complaints will be essential.

Credit reporting has undergone a significant review. This is particularly significant for merchants and traders who provide credit to customers. Both the privacy policy and Ts&Cs will require careful review to get up to date with the changing law and meet the challenges that the enhanced provisions and the increased powers of the Privacy Commissioner bring.

Enquiries into credit worthiness may become easier to make but the way in which this information can be used is being tightened. The new Part IIIA permits more comprehensive credit reporting and allows reporting of information on an individual's current credit commitments and repayment history over the previous two years. In addition a new credit reporting code (to be called the CR code) will be introduced in due course. It is intended to be developed by industry subject to approval by the Privacy Commissioner.

The increase in widening credit reporting powers is constrained by new protections for individuals. These include:

- a simplified and enhanced correction and complaints process
- a prohibition on the reporting of credit-related information about children
- a prohibition on the reporting of defaults of less than $150
- the introduction of specific rules to deal with pre-screening of credit offers
- the introduction of specific provisions that allow an individual to freeze access to their credit related personal information in cases of suspected identity theft or fraud
- the introduction of civil penalties for breaches of certain credit reporting provisions.

Credit reporters will have already commenced collecting information on individual's repayment history. This information will be licensed to providers from March 2014. Another aspect is that new terminology is used under the changes. Credit Reporting Agencies will be known as Credit Reporting Bodies.

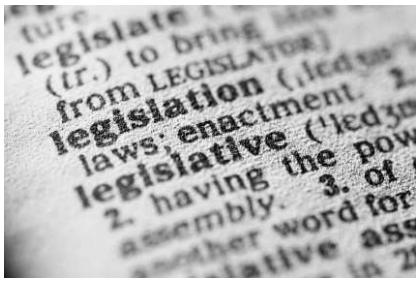
The new Australian Privacy Principles will apply to credit providers in some specific ways, with particular reference to credit information, credit eligibility information and information derived from a Credit Reporting Body. Specific, enhanced provisions will apply to consumer credit. There are specific rules dealing with the provision of repayment history information to a credit reporting body. There are specific rules regarding the use or handling of information, known as "derived information" which includes a credit score or risk assessment in relation to credit worthiness.

Increased Powers

Currently, the powers of the Privacy Commissioner are limited to making a determination that requires an apology, financial compensation or an undertaking to retrain. If this is not effective the Commissioner can take the matter to the Federal court. Under the new provisions from March 2014 the Commissioner's powers are greatly enhanced. This will include not only the ability to make a determination but also to obtain written undertakings regarding compliance with the right to enforce those undertakings in court. Significantly, the Commissioner can seek fines up to $1,700,000 for serious or repeated breaches.

The Commissioner will have the right to undertake audits of private sector organisations if that seems appropriate.

Action required



The clear message from the Privacy Commissioner is that any business that is in the habit of providing credit should be reviewing its Ts&Cs, credit policies and its privacy policy. For most organisations that give credit the privacy policy and the terms and conditions of trade are intertwined. Any changes to the company's privacy policy must be reflected in the terms of trade to ensure there is no confusion between them. Updating the privacy policy is a must, but so too is updating the company's Ts&Cs.

"Privacy and Your Clients: An Agenda for Every Business"

Tal Williams, Partner and Joann Yap, Graduate Lawyer

In the 2012-13 financial year, the Compliance Branch of the Office of the Australian Information Commissioner (OAIC) received 1496 privacy complaints, and increase of 10% over the 1357 received in 2011-12. In addition, the OAIC dealt with 13 own motion investigations and 61 voluntary data breach notifications. We discuss below one case (misuse of a mobile phone number by a bank to direct market a bank related insurance product) that may be of interest.

The case was based on an alleged breach by the bank where it used or disclosed personal information about an individual for a purpose other than the primary purpose of collection.

Facts

The complainant was a customer of a financial institution which required the complainant to provide a mobile phone number when it set up internet banking. The financial institution told the complainant that the mobile phone number would only be used in providing security identification for internet banking.

Five years later a direct marketing company made several calls to the complainant to sell insurance products on behalf of the financial institution.

The bank tried to justify use of the mobile number on the basis that it had sent the complainant a letter about its insurance products a week before the complainant received the telephone calls. A notice in fine print at the back of the letter stated that the financial institution would send the complainant's mobile phone number to the financial institution's contract company, to call the complainant, unless the complainant contacted a specified number to advise they wanted to be excluded.

Decision

The financial institution sought to rely on NPP 2.1(a), claiming that as the complainant had not responded to the letter by calling to advise they did not want to participate, the institution was entitled to assume that its disclosure of the complainant's personal information, including mobile phone number, was within the complainant's reasonable expectations.

The Commissioner found that to satisfy NPP 2.1(a): the disclosure must be related to the primary purpose for which the personal information was collected.

In this case the complainant had provided their mobile phone number for security identification purposes. The Commissioner took into account the context in which the mobile phone number was collected and took the view that the primary purpose of collection was to provide extra security protection for banking transactions, and that disclosing the mobile phone number for the secondary purpose of enabling the direct marketing company to contact the complainant was not related to the primary purpose of collection.

In accordance with NPP 2.1(a)(ii), the individual must reasonably expect the organisation to use or disclose their information for the secondary purpose.

In this case the Commissioner's view was that the complainant would not have reasonably expected their mobile phone number to be passed to a third party to conduct direct marketing, and that the complainant was unlikely to have closely read the correspondence as the letter sent by the financial institution was about a service that the complainant was not interested in receiving from that organisation.

The Commissioner also found the option to 'opt out' was not clearly and prominently presented and easy to take up. It was in fine print on the reverse of a letter. The Financial institution could not establish consent to a use or disclosure where it wishes to rely on a failure to object to such a use or disclosure.

Additionally, NPP 2.1(c), permitting use of personal information for the purposes of direct marketing, did not apply as the financial institution did not use the information itself for the purpose of direct marketing, but rather disclosed it to a third party for that purpose.

The parties conciliated the matter, and the complainant accepted a letter of apology and assurances from the financial institution that the complainant would not be included in any future marketing campaigns. The financial institution also undertook to conduct a review of its marketing campaign procedures. The Commissioner was satisfied that the matter was adequately dealt with and closed the matter.

Some may say that the financial institution got off lightly, however, businesses should be aware that possible outcomes of privacy complaints include:

- An apology;
- A change to the respondent's practices or procedures;
- Staff counselling;
- Taking steps to address the matter, for example providing access to personal information, or amending records;
- Non-financial options, for example a complimentary subscription to a service; and/or
- Compensation for financial or non-financial loss – and from March 2014 these will increase up to $350,000 for individuals and up to $1.7 million for companies.

The Privacy Act – More stringent requirements relating to direct marketing and cross-border disclosures

Tal Williams, Partner

From March 2014 there are to be more changes to the *Privacy Act 1988* which could be relevant to you and your business. You will need to consider your own privacy compliance arrangements to make sure they don't leave you at risk.

The changes are:

Australian Privacy Principles

From 12 March 2014, the amendments replace the Information Privacy Principles (IPPs - which applied to the Commonwealth and Territory public sectors), and the National Privacy Principles (NPPs - which applied to the private sector), with 13 Australian Privacy Principles (APPs) which will apply to both Commonwealth and Territory agencies and to the Australian private sector.

In summary the new APPs cover:

- 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 or disclosure of personal information
- APP 7 – direct marketing
- APP 8 – cross-border disclosure of personal information
- APP 9 – adoption, use or 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.

The APPs largely mirror the current NPPs. However, they require a much more active management of your privacy policy as it will introduce tighter controls on direct marketing and create liability for offshore breaches of privacy when data is sent overseas (cloud storage included).

Under the APPs, Commonwealth agencies and private sector organisations are required to manage personal information collection, use and disclosure in an open and transparent way. Privacy policies must be reviewed regularly and kept up to date as "living" documents.

Direct marketing

Under APP7 and the other APPs, a collecting party will be prohibited from using personal information for direct marketing (or disclosing the personal information to another organisation for use in direct marketing) unless the person:

(a) would reasonably have expected the collecting party to do so and

(b) a simple "opt out" mechanism is provided to enable the individual to stop receiving direct marketing material.

For further details, refer to page 4 in this update.

APP7 does not apply to the extent that the *Do Not Call Register Act 2006* and the *Spam Act 2003* applies, which also regulate electronic direct marketing.

As with all privacy issues, it is always best to seek and obtain express consent from the individual. Assuming it will be okay to direct market will is no longer be acceptable.

Increase in the powers and functions of the Australian Information Commissioner

The amendments clarify the powers and functions of the Australian Information Commissioner in the development and registration of APP Codes of Practice, it will also improve the Commissioner's ability to promote compliance with privacy obligations. Civil penalties of up to $340,000 for individuals and $1.7 million for companies are possible where there is a serious or repeated breach of privacy.

The Commissioner will be able to audit compliance, initiate investigations and make enforceable determinations. The Commissioner will also be able to accept written undertakings from organisations that they will take, or refrain from taking, action to ensure compliance with the Privacy Act.

Cross border disclosure of personal information

As discussed in more detail in this update, the amendments impose greater obligations on entities who disclose personal information about an individual to an "overseas recipient". Disclosure could means storing data "on the Cloud" where the cloud service is located outside Australia. Entities must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information (subject to specified exceptions). The party that discloses the personal information to the overseas entity will be liable under Australian privacy law for breaches of the APPs committed by the overseas entity.

Where a business sends personal information (including health information) to organisations overseas (for example for reporting of tests, records management or marketing), it must ensure that exemptions apply or the person from whom that information is collected is expressly aware of and

consent to this. More detailed information will also need to be included in a business' corporate privacy policy.

Bearing in mind these changes it is likely that additional provisions will need to be inserted in your privacy policy, and your data collection processes reviewed. Greater attention will also need to be paid to ensure you have the consent of people on your database to use their data in the way you propose.

Australian Privacy Laws and Health Information

Alison Choy Flannigan, Partner

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;
- the collection of family, social and medical histories; and
- 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.
- 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).

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

Alison Choy Flannigan, Partner

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 29 October 2013:

- The total number of people who registered for an eHealth record as at 29 October 2013 was 1,042,966.
- More than 5,681 healthcare provider organisations have signed onto the eHealth Record system.
- 8,105 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.

With respect to the number of providers with HPI-Is that have been linked to access the system, it is NeHTA's understanding that these numbers are linkages via the provider portal and exclude any linkages through local clinical information systems, so the total number of authorized users can be significantly greater.

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. A consumer request to withhold information or remove information is never flagged unless it is specifically indicated in the record by agreement between the consumer or clinician.

- 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 may be under a common law 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 the clinician should use their professional judgment to not upload such information 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.

KEY CONTACTS FOR THE BUSINESS CORPORATE & COMMERCIAL GROUP

Jonathan Casson
Partner
T: +61 2 9390 8340
jonathan.casson@holmanwebb.com.au

Tal Williams
Partner
T: +61 2 9390 8331
tal.williams@holmanwebb.com.au

David Pyne
Partner
T: +61 7 3235 0116
david.pyne@holmanwebb.com.au

Tim Smyth
Special Counsel
T: +61 2 9390 8342
tim.smyth@holmanwebb.com.au

Sandra Ivanovic
Senior Associate
T: +61 2 9390 8352
sandra.ivanovic@holmanwebb.com.au

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

Corinne Attard
Partner
T: +61 2 9390 8354
corinne.attard@holmanwebb.com.au

Craig Singleton
Partner
T: +61 7 3235 0105
craig.singleton@holmanwebb.com.au

Venus Amoro-Njuguna
Senior Associate
T: +61 2 9390 8308
venus.amoro-njuguna@holmanwebb.com.au

Making further external recognition of Holman Webb's legal expertise, we are pleased to advise of our inclusion in the Commonwealth Government's Legal Services Multi-User List (LSMUL). Holman Webb was appointed in the areas of Government and Administration Law and Corporate and Commercial Law.

Holman Webb
Lawyers

Sydney

Level 17 Angel Place
123 Pitt Street
Sydney NSW 2000
T:+61 2 9390 8000
F: +61 2 9390 8390

Melbourne

Level 10
200 Queen Street
Melbourne VIC 3000
T:+61 3 9691 1200
F: +61 3 9462 3183

Brisbane

Level 13
175 Eagle Street
Brisbane QLD 4000
T:+61 7 3235 0100
F: +61 7 3235 0111

www.holmanwebb.com.au