ThomsonsLawyers

Health Alert

November 2011

Health information in a cloud - is it all blue skies and clear flying or are there storms ahead?

Background

The term 'eHealth' means the 'combined use of electronic communication and information technology in the health sector'.[1]

Cloud computing is the provision of computing services over the internet from a remote location, rather than services from a desktop, laptop, in-house server, local areas network, smart phone, tablet or other mobile device. As an alternative to providing services in-house, the individual or organisation will contract with a provider for the delivery of applications and storage via the internet. In short, provided internet access is available, computer applications and information are available to the user regardless of where they are physically located.

In the last edition of the Health Alert, we reported on the draft eHealth records legislation and the proposed personally controlled electronic health record (**PCEHR**) system. The proposed PCEHR system, encompassing eHealth, aims to provide patients and their medical advisers with internet access to their health records. The government claims that the proposed PCEHR system will protect individual privacy through legislation, technical security and access controls. Access to records will only be available to health care providers and those that are authorised to have access to an individual health identifier and the associated PCEHR.[2]

Health information is, by its very nature, sensitive. It also has a value to other people (not always with the best of intentions). While there is no doubt the Government is dedicating resources to ensure it protects eHealth records, there are still substantial risks that must be considered by those accessing the PCEHR system to ensure the on-going protection of the data.

Privacy considerations

Each of the health professionals and health organisations (e.g. doctor, hospital, aged care or other health facility, pharmacist and other allied health professionals) legitimately accessing the PCEHR system will be themselves subject to privacy and confidentiality obligations to the patient.

Holders of the information therefore have a duty to implement their own safeguards in respect of the PCEHR and related information and not only rely upon the identifiers or systems put in place by the Government.

Once information in connection with a PCEHR is accessed or created, the health professional or organisation obtaining or creating that medical information will have to store that information. Almost inevitably this medical information, in whole or in part, will ultimately be stored by way of the cloud computing environment at some part of the chain of creation and use.

In the cloud computing environment, often the 'owner' or 'holder' of the data will not know the physical location of the information which may or may not be within Australia. However, the National Privacy Principles (under section 14 of the *Privacy Act 1988* (Cth) which have broad application in the health care environment), impose restrictions on an organisation's ability to send personal

[1]www.ehealthinfo.gov.au/what-is-ehealth

[2]http://health.gov.au/internet/main/publishing.nsf - Health Identifiers Service – Frequently Asked Questions.

information (including health information) outside of Australia, including for example obtaining the specific consent of the individual. It is important to remember that different countries have their own regimes in respect to the protection of personal information which will not necessarily be equivalent to the regime in place in Australia or in the relevant Australian state or territory.

Accessing, using and storing medical and eHealth records

The Commonwealth Government is proposing significant security measures in respect of the PCEHR system which it will control. It therefore seems likely that other parties attempting to illegally access information held in or related to the PCEHR system will concentrate their efforts on the systems of individual health professionals or health organisations other than the Government. Health professionals and health organisations, even those electing not to utilise a 'cloud computing' system, must therefore be vigilant and implement appropriate strategies to protect the eHealth and related information which they access, hold or control.

At any point, where the information held about a person in the PCEHR system is accessed and then used, the information may be compromised unless appropriate security systems are in place in respect of each access and use.

There are unlimited scenarios to consider where a health professional or health organisation may access information held in the PCEHR system and use it in a way which will not necessarily be protected by the security measures imposed or envisaged by the Government. For example, a doctor attending a hospital to provide health care to patients will access information created and/or obtained by that hospital through the PCEHR system and which the hospital makes available to the doctor. That doctor may also have access to the information on the basis of their own identifiers but may transfer all or some of the information, either directly or by way of their notes, onto a laptop or via email or other mobile device. Similar circumstances may arise in the context of a doctor or allied professional working in a travelling capacity (e.g. home visits or visits to an aged care or other health facility) or rural environment and accessing records by way of the internet or with a general practitioner treating a patient who has just been in hospital.

As we mentioned in our last edition of the Health Alert, there is the potential for both civil and criminal penalties to be imposed as relevant on individuals or organisations in connection with the PCEHR system. In addition, in any scenario where information in the PCEHR system is found to have been accessed or used by an unauthorised third party, there is likely to be significant fall-out and reputational damage to all members of the 'chain' of creation and use of the information. This is especially so if it is not possible to identify all of the points of access or which of the hospitals, aged care facilities or health professionals who had access was the source of, or created the opportunity for, the unauthorised access or use of the health information.

Security

Security of information from various sources stored in the cloud computing environment poses complicated security issues. While due diligence at the time of contracting with a service provider will be essential, by its very nature once information has been transferred to the cloud environment, the source organisation has significantly reduced ability to audit where the information is located and the way the information is being managed and protected.

While obligations of privacy, confidentiality and security can be contractually (or even legislatively) imposed on providers of cloud computing services, the duties of the source organisation in relation to the information, which that organisation chooses to store information in the cloud computing environment, cannot simply be abrogated by attempts to contractually or otherwise pass the liabilities and responsibilities for the information to other parties. The challenge, then, is for the source organisation to establish, implement and maintain processes through which the source organisation can conduct ongoing audits of the activities of the provider of the cloud computing services such that all parties will be subject to good governance and oversight.

It is important that each 'owner', 'holder' or 'user' within the PCEHR system be in a position to provide evidence of implementation and maintenance of appropriate security measures, not only in respect of their own storage, access and use of the information, but also in respect of the processes implemented for providing access to the information by any third party.

An over the counter or over the internet security software package may not be sufficient to protect access, storage and use of information sourced from the PCEHR system and, in any event, needs to be regularly updated and upgraded to protect against new viruses and attacks to the integrity of the computer's security.

ThomsonsLawyers

In the context of the provision of back up services provided by third parties, security issues arise which are similar to those for other aspects of managing information electronically. The source organisation must be across what backup systems are in place, what service providers are involved in providing the backup systems, and how those systems are secured and available to the source organisation as and when required.

Considerations

Take a 'whole of life' review of the project. For example, while cloud computing offers attractions in terms of cost, these cost savings may be far exceeded by reputational damage, compensation and investigative costs if the data is accessed unlawfully. The review should therefore consider what services may be appropriately delivered through cloud computing, with more sensitive data firewalled within the organisation itself.

When entering into an agreement which will include the provision of cloud computing services, the simple questions to ask as a starting point are:

- How is the organisation's information, data and applications being stored, accessed and used?
- Are the ways in which the organisation's information is being stored, accessed and used appropriately protected?
- If other parties are engaged to provide aspects of storage and/or security, how can access by the organisation to its own information be guaranteed as required, including in an emergency situation?

Key points regarding eHealth security and cloud computing

- Establish, implement and maintain risk assessments and controls which take into consideration the particular challenges and risks with accessing, storing, transmitting and using eHealth information.
- Engage specialist services providers for computer security (including back up) and ensure there is an ability to conduct audits and require updates.
- If cloud computing services are used, choose what parts of the commercial and other operations of the organisation are most efficiently serviced through cloud computing and firewall the remaining operations and information of the agency. Cloud computing should not be considered as a 'whole of operation' option.
- When engaging information technology service providers, include as key selection criteria during the procurement process: requirements for the provider to show evidence of its security processes and processes for access by the source organisation to its systems to enable audit by the source organisation of the on-going compliance and effectiveness of its systems.
- Consider carefully any exclusion or limitation of liability and obtain appropriate indemnities when contracting with information technology service providers. For example, it is common in contracts prepared by the service providers to exclude 'consequential' or 'indirect' losses or limit damages to replacement or re-performance of the services. However, before this is agreed, consider what the particular risks and losses are likely to be and only then agree to **any** level of loss limitation or exclusion.

Kathie Sadler
Special Counsel
+61 7 3338 7515
ksadler@thomsonslawyers.com.au

Charities and not-for-profit update

Recently, the Commonwealth Government released a number of documents affecting charities and some other not-for-profit **(NFP)** entities.

Charities taxation ruling

On 12 October 2011, the Australian Taxation Office **(ATO)** released Taxation Ruling TR 2011/4 Income tax and fringe benefits tax: charities.

This ruling explains the ATO's view of the meaning of 'charitable' for the purposes of the terms 'charitable institution' and 'fund established for public charitable purposes' where they are used in the income tax and fringe benefits tax legislation.

The ruling applies to income years starting both before and after its date of issue. It replaces TR 2005/21, and finalises Draft Taxation Ruling TR 2011/D2.

In finalising the ruling, the ATO made some changes from the draft. For example, the ruling now expressly indicates that a charitable institution that 'endeavours to make a profit from its activities can still be charitable if its profit making goal is only in aid of its charitable purpose'.

The ATO also issued the Ruling Compendium, which is a compendium of responses to the issues raised by external

parties to draft Taxation Ruling TR 2011/D2.

Click here for Taxation Ruling TR 2011/4 and the Ruling Compendium.

NFP Newsletter – Issue 1

On 14 October 2011, the Treasury released a new NFP newsletter.

The newsletter looks at the following topics:

- An overview of the NFP reform agenda
- Better targeting of tax concessions
- Treasury's role in the reform process
- The Implementation Taskforce
- What's happening in the next month
- What's coming up in the next 12 months.

The Treasury outlined the timetable for public consultations as follows:

- Introducing a statutory definition of 'charity': consultation paper – October 2011 (see below)
- Second exposure draft of 'In-Australia' special conditions and definition of not-for-profit: expected late 2011
- Better targeting of tax concessions: exposure draft – expected late 2011
- A national approach to fundraising regulation: discussion paper – expected late 2011
- Legislation to establish the new Australian Charities and Not-for-profits Commission (ACNC): exposure draft – expected late 2011
- Review of corporations limited by guarantee and governance arrangements for NFPs - expected late 2011
- Introducing a statutory definition of 'charity': exposure draft legislation – expected first half of 2012.

Click here for the NFP newsletter – Issue 1.

Consultation Paper – A Definition of Charity

On 28 October 2011, the Treasury released a Consultation Paper on the proposed definition of charity, as part of a consultation process to provide interested parties with an opportunity to comment.

The Commonwealth Government announced in the 2011-12 Budget that it would introduce a statutory definition of charity.

The Consultation Paper outlines the background to a statutory definition, including previous recommendations and inquiries, as well as developments that have occurred since the Commonwealth Government released the 2003 consultation package on a charity definition.

It is proposed that the statutory definition of charity will:

- apply for all Commonwealth laws;
- take effect from 1 July 2013; and
- be based on the 2001 *Report of the Inquiry into the Definition of Charities and Related Organisations*, the definition in the Charities Bill 2003, and taking into account of the findings of recent judicial decisions such as *Aid/Watch Incorporated v Commissioner of Taxation*.

The core definition in the Charities Bill 2003 contained the following broad elements that an entity must meet to be a charity:

- the entity is a not-for-profit entity;
- it has a dominant purpose that is charitable;
- it is for the public benefit;
- it does not engage in activities that do not further, or are not in aid of, its dominant purpose;
- it does not have a disqualifying purpose;
- it does not engage in, and has not engaged in, conduct that constitutes a serious offence; and
- it is not an individual, partnership, a political party, a superannuation fund or a government body.

From 1 July 2012, ACNC will register new charities based on the current law. Existing charities that were endorsed by the ATO as income tax exempt will be transitioned to the ACNC at 1 July 2012, and will not need to re-register.

From 1 July 2013, ACNC will register new charities based on the new statutory definition of charity. Charities remain responsible for self-assessing their eligibility on an ongoing basis. The ACNC will review existing registrations over time.

The ATO will accept the ACNC's registration of charitable status, but will retain responsibility for determining eligibility to access Commonwealth tax concessions which are subject to special conditions.

The process for consultation on the statutory definition of charity is as follows:

ThomsonsLawyers

- Submissions on the consultation paper are due 9 December 2011.
- The Government will also consult on exposure draft legislation (expected in first half of 2012).
- Introduction of draft legislation into Parliament expected in mid-2012.
- Guidance on new statutory definition will be issued by the ACNC following passage through Parliament.
- The definition will come into effect on 1 July 2013.

Click here for the Consultation Paper, and the Treasury's NFP Reform Factsheet.

If you would like us to assist you with making submissions to the Treasury, please contact us

Philip De Haan
Partner
+61 2 9020 5703
pdehaan@thomsonslawyers.com.au

Yat To Lee
Senior Associate
+61 2 9020 5742
ylee@thomsonslawyers.com.au

Communicating electronically – when is email ok for formal contractual notice?

The health and aged care sectors are not alone in relying heavily on electronic communication for sending and receiving information on all manner of subjects. However, it is important to think carefully before using email for notices under contracts.

Organisations work with a wide range of contract documents many of which are the subject of standard printed conditions and are managed by business managers without specific involvement of senior management. However, power to give approvals, execute documents and make decisions which bind an organisation will often be restricted to those persons with relevant internal authorisations. Formal notifications under contracts are not just limited to things like termination, renewal of exercise of options and can have significant financial consequences for the organisation, so it is important to get the process right for issuing and receiving notifications.

Under section 9 of the *Electronic Transactions Act 1999* (Cth) and similar state and territory legislation, there are two conditions that must be fulfilled before information sent by email or other electronic communication is valid. First, the information must be kept in such a way that it is reasonable to expect that it could be accessed and therefore useable for subsequent reference and secondly, the recipient of the information must consent to the information being delivered by means of an electronic communication.

Not having a piece of paper with a traditional handwritten signature is not a bar to using email for formal notice (or even execution) in contracts – a signature can be applied by mechanical means and does not have to look handwritten. However:

- For contracts that have no express provision for notices to be sent by email it is highly unlikely, in the absence of express consent of the recipient party, that courts would treat an emailed notice as valid. The safest course is to use a method of delivery specified in the contract. If an organisation is willing to send and receive notices under contracts by email this is best dealt with at the time of negotiating the contract and it should be expressly included in the notice provisions.
- Even where electronic communication is specifically allowed in a contract, it may still be safer to use fax which is easier to prove it was sent and received and fax numbers usually relate to an organisation. In addition there is a potential practical problem with email as most email addresses are personal to a particular individual. This may result in issues arising out of failure of the recipient to actually see the notice because of temporary absences, for example annual leave, or where a person has left an organisation and notice details have not been updated.

Key issues for electronic notice in contracts:

- If your organisation wants to ensure that notices sent by email are valid and enforceable, express provision to that effect should be included in the contract.
- Care should be taken to ensure practical issues regarding actual receipt are addressed, for example, by investigating opportunities for creating a 'central' email address or ensuring that processes are in place to manage email addresses for persons with particular notice delegations, including 'out of office' notifications or automatic forwarding when absent on leave or at exit from organisation.

Jim Baillie
Special Counsel
+61 2 9020 5746
jbaillie@thomsonslawyers.com.au

ThomsonsLawyers

Legislation Update

Commonwealth Legislation

National Health Reform Amendment (National Health Performance Authority) Act 2011 (Cth)

This Act was assented to on 14 October 2011.

The Act amends the *National Health and Hospitals Network Act 2011* (Cth) **(principal Act)**.

The Act establishes the National Health Performance Authority **(Performance Authority)**.

Specifically, the Act:

- substitutes the title of the principal Act to the "National Health Reform Act 2011";
- makes various minor amendments to include references to the Performance Authority, and to include a number of new definitions related to the Performance Authority;
- makes amendments relating to the Australian Commission on Safety and Quality in Health Care ("the Commission") to distinguish between provisions relating to the members and Chief Executive Officer of the Commission and the Performance Authority, and to introduce provisions relating to secrecy and disclosure of information by the Commission; and
- makes other miscellaneous amendments.

Health Insurance (Diagnostic Imaging Services Table) Regulations 2011 (Cth)

These Regulations have been made under the authority of the *Health Insurance Act (1973)* (Cth).

According to the explanatory statement, the Regulations repeal the *Health Insurance (Diagnostic Imaging Services Table) Regulations 2010* (Cth) and prescribe a new diagnostic imaging services table for the 12 month period commencing 1 November 2011.

Health Insurance (Pathology Services Table) Regulations 2011 (Cth)

These regulations have been made under the authority of the *Health Insurance Act (1973)* (Cth).

According to the explanatory statement, the purpose of the Regulations is to replace the *Health Insurance (Pathology Services Table) Regulations 2010* (Cth), and prescribe a new pathology services table for the 12 month period commencing on 1 November 2011, including to set out items of pathology services which are eligible for Medicare benefits, the amount of fees applicable in respect of each item and rules for interpretation of the table.

Health Insurance Amendment Regulations 2011 (Cth)

These Regulations amend the *Health Insurance Regulations 1975* (Cth).

According to the explanatory statement, the amending Regulations "facilitate the implementation of the 'changes to fees for fully depreciated diagnostic imaging equipment' or the Capital Sensitivity 2009-10 Budget Measure".

Specifically, the amending Regulations amend r. 20C (Primary information - types of diagnostic imaging equipment), including to:

- prescribe various types of diagnostic imaging equipment, to "encourage diagnostic imaging service providers to upgrade and replace aged equipment as appropriate"; and
- define "2011 Determination" and "upgraded".

The amending Regulations will commence on 25 October 2011.

Health Insurance Amendment Regulations 2011 (Cth)

These Regulations amend the *Health Insurance Regulations 1975* (Cth).

According to the explanatory statement, the amending Regulations:

- update Sch. 6 (Services for which Medicare benefit is 100% of Schedule fee), by omitting and substituting various items; and
- correct a minor drafting error in that Schedule.

Health Insurance (General Medical Services Table) Regulations 2011 (Cth)

These Regulations have been made under the authority of the *Health Insurance Act 1973* (Cth).

According to the explanatory statement, the Regulations prescribe a new table of general medical services for the 12 month period beginning on 1 November 2011, as a consequence of the repeal of the *Health Insurance (General Medical Services Table) Regulations 2010* (Cth).

Specifically, the new General Medical Services Table:

- increases the fee for most items by 2%;
- omits and includes various new items; and
- makes minor amendments to the descriptors for several items and other consequential amendments.

The Regulations will commence on 1 November 2011.

New South Wales Legislation

Work Health and Safety Legislation Amendment Bill 2011 (NSW)

This Bill proposes to amend the legislation listed below. The Bill was introduced into the Legislative Council and received its second reading speech on 20 October 2011.

The Bill would make various amendments as a consequence of the enactment of the proposed Act and the *Work Health and Safety Act 2011* (NSW) including to update references to the *Occupational Health and Safety Act 2000* (NSW) with references to the *Work Health and Safety Act 2011* (NSW) and update certain specific terms.

This affects the following legislation:

- Health Services Act 1997 No. 154
- Licensing and Registration (Uniform Procedures) Act 2002 No. 28
- Radiation Control Act 1990 No. 13
- Smoke-free Environment Act 2000 No. 69

Children (Education and Care Services) Supplementary Provisions Bill 2011 (NSW)

This Bill proposes to amend the legislation listed below. The Bill was introduced into the Legislative Council and received its second reading speech on 20 October 2011.

According to the explanatory note, the objective of the Bill is to provide for the regulation of certain children's education and care services that are not subject to the *Children (Education and Care Services National Law Application) Act 2010* (NSW) and align the regulation of those services, where practicable, with that Act. The children's education and care services that are subject to the proposed Act consist of home based education and care services, other than family day care services, and mobile education and care services, centre based education and care services, and other education and care services of a kind prescribed by the regulations.

Specifically, the amending Bill would make minor consequential amendments relating to the repeal of Chapters 12 and 12A of the *Children and Young Persons (Care and Protection) Act 1998* (NSW), the commencement of the National Law and the enactment of the proposed Act.

This affects the following legislation:

- Public Health Act 1991 No. 10

For further information, please contact:

Lucinda Smith
Partner
+61 2 9020 5748
lsmith@thomsonslawyers.com.au

Jim Baillie
Special Counsel
+61 2 9020 5746
jbaillie@thomsonslawyers.com.au

Ken Ramsay
Consultant
+61 2 8248 3460
kramsay@thomsonslawyers.com.au

Kathie Sadler
Special Counsel
+61 7 3338 7515
ksadler@thomsonslawyers.com.au

Samantha Culshaw
Senior Associate
+61 2 9020 5712
sculshaw@thomsonslawyers.com.au

Marc Wyld
Senior Associate
+61 2 9020 5708
mwyld@thomsonslawyers.com.au

Ruth Hood
Associate
+61 2 8248 3459
rhood@thomsonslawyers.com.au

Sophie Parker
Lawyer
+61 2 8248 3403
sparker@thomsonslawyers.com.au