HealthLEGAL
www.healthlegal.com.au
August 2016 Edition

Health Privacy in a Big Data World

By Claudia Hirst, Legal Counsel and Giovanni Marino, Senior Solicitor

Introduction

The consultation draft of the 'Guide to Big Data and the Australian Privacy Principles' (**Guide**) was released by the Office of the Australian Information Commissioner (**OAIC)** in May**.** The consultation period closed in July and we can expect a finalised Guide in the coming months. It is therefore timely to consider some of the key concepts in the big data and privacy conversation and how they apply to health services.

Message – Design, Management, and Improvement

Privacy is evolving quickly as big data capacity grows. The OAIC recommends that organisations adopt a design and systemic risk management approach. Tools to assist with this approach are:

- A privacy management plan
- Privacy Impact Assessments
- Privacy notices which are appropriate for purpose
- Security risk assessments
- Continuous quality improvement.

What is Big Data?

Big data is the collection, creation and fast analysis of large amounts of personal data. In the health sphere, it has developed as a result of the move from paper based to electronic health records coupled with the expansion in data analytics technology. In simple terms data analytics technology uses algorithms to rapidly sort, collate, compare and analyse vast amounts of data.

The Guide refers to Gartner's 'three V's' definition of the term 'big data':

> … high-volume, high-velocity and/or high-variety information assets

How is it Relevant to Health Services?

Uses of big data range from large scale research on the cause of diseases to the development of patient centred applications which feedback intelligence to patients allowing them to self-monitor progress and report it through mobile apps.

Smaller organisations or service providers may not be in the business of analysing big data. However, such organisations are still the repositories of large amounts of 'liquid' patient data. One way for smaller organisations to leverage the information pool is through partnerships with larger or multiple organisations.

The challenge for health services in this environment is to contribute to and benefit from big data analytics while still protecting genuinely sensitive and identifiable information.

Legislation and the Guide

The *Privacy Act 1988* (Cth) (**Act**) and its Principles (**APPs**) apply to private health care organisations, community health centres, and other private health providers. Similar principles apply to public health services under State and Territory health records legislation.

Big data activities challenge how the key requirements for collection and handling of personal information under privacy principles work in practice. The Guide provides a structure for working through this challenge and will also be useful to entities not bound by the APP's.

Following are some of the key messages from the Guide in its current draft form.

Privacy by design

The Guide recommends Privacy by Design (**PbD**). Privacy by Design means building privacy into the architecture of systems and business practices rather than "bolting it on afterwards" – it means embedding privacy into organisational governance.

> Embedding 'privacy by design' will lead to a trickledown effect where privacy is considered automatically by the entity, resulting in better overall privacy practice and compliance.

Important features of PbD are:

- A privacy officer
- Strategic documents which acknowledge systemic privacy management
- A privacy management plan
- A risk management and mitigation approach to privacy.

Privacy Impact Assessments

Privacy Impact Assessments (**PIAs**) are an essential tool for implementing PbD.

A PIA systematically assesses the impact of a project or function on individual privacy and recommends design that manages that risk by eliminating or minimising it. A PIA will consider system functionality as well as communication with clients and patients.

> Undertaking PIAs for big data activities will help entities describe their aims and the key privacy impacts for the activity.

The OAIC *Guide to undertaking privacy impact assessments* can be found at www.oaic.gov.au.

Four elements are crucial in assessing and managing the privacy impact of business practices:

- privacy notices
- de-identification
- consent
- security.

Privacy Notices

APP 5 requires an organisation to take reasonable steps to notify individuals of the details of the collection and uses of the information – this is usually achieved through a privacy notice.

Research shows that many people do not read privacy notices. Therefore, the PIA should carefully consider the design of the privacy notice. The privacy notice should be in an easy-to-read, user centric format, tailored to its purpose.

> Privacy notices have a big job to do. They need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful.

The Guide recommends innovative approaches to privacy notices:

- 'just in time' or video privacy notices that appear on screen when an individual is about to input their personal information
- multi-layered privacy notices, for example, using brief notices supplemented by longer notices.

Consent

APP 6 requires that health information held by an organisation only be used or disclosed for its primary purpose. However, it may be used or disclosed for a directly related secondary purpose in specified circumstances, including where:

- the individual has consented; or
- the individual would reasonably expect the organisation to use the information for the secondary purpose, and that purpose is related (or directly related in the case of health information) to the primary purpose for which the information was collected.

The privacy notice may be a key document in establishing express or implied consent.

If an organisation plans to use or disclose personal information for a 'secondary purpose' this should be included in the privacy notice.

A privacy notice may set out a range of likely secondary uses of personal information, including big data activities. This will inform individuals of what to expect.

The Guide recommends that organisations consider how they might allow individuals to choose which uses and disclosures they agree to and which they do not – for example, by using a multi-tiered approach.

Many uses of big data are as yet unknown. One way to address this is to allow for recontact of individuals whose information is collected. Another option is to utilise de-identified data.

Research

Organisations involved in conducting research relevant to public health or public safety, or in the management, funding or monitoring of a health service, will be aware of the *Guidelines approved under Section 95A of the Privacy Act 1988* (the **Guidelines**). The Guidelines provide a framework to ensure the protection of an individual's health information that is collected, used or disclosed in the conduct of research or health service management activities. The Guidelines require that it must be impracticable to seek consent from the individual involved for the organisation to collect, use or disclose health information, and also that de-identified information will not achieve the purpose of the research or health service management activity.

A PIA may overlay and complement the requirements in the Guidelines to ensure that a research or health service management activity protects an individual's privacy.

De-identified Personal Information

De-identified information can be used, analysed and shared without compromising a person's privacy. The Guide recommends that entities consider first whether de-identified personal information could be utilised for the proposed purpose.

De-identification is no longer as simple as removal of names and file numbers and address details. As capacity for data analytics grows, the potential for re-identification also grows. Matching of data sets between providers may result in re-identification of data that was de-identified in the individual data set.

> Big data analytics can lead to the creation of personal information

The Guide recommends that the PIA examine:

- the proposed de-identification techniques used
- how the de-identified data will be handled (for example, whether the data will be disclosed to third parties)
- the risk of re-identification.

The intended outcome will be the adoption of strategies to achieve effective de-identification, recognition of potential re-identification risks and management of those risks.

Security of Personal Information

Overseas disclosure will occur if an organisation engages overseas cloud service providers to manage data.

Before disclosing information overseas, APP 8.1 requires an organisation to take reasonable steps to ensure that the overseas recipient does not breach the APPs.

Big data activities often hold larger amounts of data and for longer periods of time.

APP 11 requires organisations to take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

> …'honey pots' containing vast amounts of valuable data may increase the risk that an entity's information systems may be hacked.

The Guide recommends that an information security risk assessment be part of a PIA.

A security risk assessment will identify 'reasonable steps' to protect personal information. These may include:

- providing access on a 'need to know' basis
- maintaining an audit log of ICT system activities to detect and investigate privacy incidents
- encryption and intrusion prevention and detection systems
- destroying or de-identifying the personal information when it is no longer needed
- having a response plan in the event of a data breach.

If you have any questions arising out of this article, please contact ***Giovanni Marino*** *on* ***(03) 9865 1339*** *or email* ***giovanni.marino@healthlegal.com.au****.*