GILBERT
+TOBIN

HOW DO I MANAGE RISKS WHEN UNLOCKING THE POTENTIAL VALUE OF HEALTH DATA?

2019

GTLAW.COM.AU

CONTENTS

GILBERT +TOBIN

WE'RE IN THE DIGITAL REVOLUTION

While there has been a trend towards decluttering our homes with the KonMari Method™, the opposite has been happening with data – the amount of data that is tracked, collected, stored and transferred online is growing exponentially. This is one of the effects of the digital revolution – which has seen digital technology transform how people live, work and interact. The health sector is no exception to this transformation.

Historically, health data has typically been generated from sources such as doctors' notes, hospital records, clinical trials, medical imaging, prescription records and insurance claims. However, the digital age has seen the growth of new sources - such as personal health apps, wearable tracking devices, digital health service platforms and customer loyalty schemes. This has resulted in a significant increase in the volume of health data. Accenture has predicted that this volume will triple from 2017-2020.

The growth in health data has coincided with the following trends.

1. COMPANIES UTILISING EXISTING DATA TO IMPROVE BUSINESS OPERATIONS, FOR EXAMPLE TO INCREASE SALES OR EFFICIENCY.

This is particularly true of companies who are able to utilise decades of data and existing consumer databases such as pharmaceutical and insurance companies.

+ Novartis is embracing digital and data as a top priority according to Chief Medical Officer John Tsai. He has said that the company has "two million patient-years' worth of data here, collected over 20 years... sitting in little spreadsheets all over the place," said Tsai. "What we've done now is bringing them all together into one searchable database that is going to be accessible to scientists at Novartis so that they can start asking questions of the information we don't actually know we have."
+ Ascension, a leading non-profit healthcare organisation in the US, has partnered with Google to improve the delivery of its services. The collaboration (known as "Project Nightingale") will involve Ascension's infrastructure transitioning onto Google Cloud, Ascension using Google's productivity and collaboration tools and Ascension exploring artificial intelligence and machine learning .

2. NON-HEALTHCARE COMPANIES CHOOSING TO ENTER INTO THE HEALTH SECTOR.

We have observed a number of data-rich technology companies entering the health sector.

+ Apple has made health and wellbeing one of its key strategies by offering the Health app and wearable devices such as the Apple Watch to enable consumers to track health metrics such as physical activity, mindfulness and sleep. Apple has also launched software developer kits that allow third parties to develop apps to monitor patients using sensors and tools built into the iPhone. For example, the Butterfly Network has utilised this technology to turn the iPhone into a portable ultrasound device.

- Last year, Google brought all of its teams working on emerging technologies and opportunities in the health sector under "Google Health", headed by Dr David Feinberg. Google has also hired Dr Karen De Salvo as its first Chief Health Officer. In November 2019, Google announced a $2.1 billion acquisition of Fitbit, one of the most popular wearable devices for tracking health and fitness goals.
- Amazon has launched "Amazon Care" for its employees in Seattle. Amazon Care will provide digital and face to face health services by combining an app for video calls and text chats with doctors or nurses with visits from mobile care nurses. In October 2019, Amazon acquired Health Navigator which provides triaging technology that can be integrated into other digital health services.

3. COMPANIES EXTRACTING NEW VALUE OUT OFHEALTH DATA. FOR EXAMPLE, BY SELLING IT ON TO THIRD PARTIES.

- Validic is a company active in the health data marketplace, having assembled a health data platform by collating participant-generated data ranging from weight data to diabetes and nutrition data. The company collates this data from personal in-home medical devices and wearables, selling it to customers that range from hospitals to IT companies and pharmaceutical companies.
- Philips has teamed up with Validic to integrate personal health data from third-party devices and apps into Philips' digital platform to power connected health solutions and services for consumers.

4. COMPANIES STARTING TO USE ARTIFICIAL INTELLIGENCE (AI) FOR ADVANCED ANALYTICS OF HEALTH DATA.

AI and analytic tools require vast and diverse data sets to develop algorithms.

- In October 2019, Novartis announced a five-year strategic collaboration with Microsoft, where Microsoft will develop new AI tools to apply across Novartis' pharmaceutical business.
- Also in October 2019, the Australian CSIRO became the first public sector organisation in the world to market and sell a health product on Amazon. The product, Variant Spark, is targeted towards researchers and uses AI to locate genes that might cause diseases such as diabetes and Alzheimer's.

With healthcare and non-healthcare companies increasingly seizing opportunities presented by health data – what are the risks in doing so? We explore these in this publication.

WHAT IS HEALTH DATA?

Given the sensitivity of health information, its collection, use and management is regulated by the *Privacy Act 1988* (Cth) (**Privacy Act**) as well as various state-based health records legislation.

Health information includes:

- information or an opinion about an individual's health or health services provided (or to be provided);
- any personal information collected to provide or in providing a health service to an individual (including organ donation); and
- genetic information about an individual that is in a form that could be predictive about the health of an individual (or a relative).

Health information exists in many forms (some of which you may not expect) including:

+ records of the gym classes attended by an individual;
+ any records that contain an individual's healthcare identifier number (e.g. billing records and insurance records);
+ data entered into a health and fitness, diet or sleeping app;
+ data collected by wearable devices such as Fitbits, Apple watches and sleep devices that monitor health indicators and activities; and
+ medicare billing information held by an insurance provider or debt collector.

MANAGING THE RISK OF UNAUTHORISED DISCLOSURE

An organisation's failure to obtain adequate consent, implement appropriate data management processes and securely manage the health information it collects can result in serious consequences. As a result of data breaches, businesses could:

- **be subject to regulatory investigation and incur fines and penalties** – Under the Privacy Act, penalties for serious breaches can be up to $2.1 million (for body corporates). Following the Australian Competition and Consumer Commission's (**ACCC**) Digital Platforms Inquiry Final Report published July 2019 (**DPI Final Report**), data breaches may also constitute a breach of the Australian Consumer Law, which has its own separate penalty regime.
- **be subject to a class action** – For example, former and current employees of NSW Ambulance have launched a class action after a former contractor allegedly sold 130 former and current employees' workers compensation files (including medical records) to personal injury lawyers (**Ambulance Class Action**). A representative class action has been launched **against Facebook** for compensation alleging privacy breaches following the Cambridge Analytica incident.
- **sustain reputational damage**
- **incur significant remediation costs**
- **breach contracts**
- **breach director duties**
- **breach continuous disclosure obligations**
- **lose customers**

Given these significant consequences, businesses dealing with health information should ensure they have appropriate systems and practices in place for the collection, use and disclosure of the health information they collect.

Potential duty of care?

A failure to meet industry standards could also give rise to a breach of a potential duty of care by the data collector, storer and/or discloser. While this appears to be untested in Australia, claims in tort for unauthorised access and misuse have been run successfully in other common law jurisdictions. The biggest hurdles would be in demonstrating:

- that where a duty of care can be established, there is a particular standard of care and that standard has not been met; and
- loss as a result of the unauthorised access or misuse.

To protect against unauthorised disclosure, ask yourself these three questions.

1. **Consent:** Do you have adequate consent to collect, use and disclose health data for this purpose?
2. **Data Systems:** Do you have appropriate data management systems in place?
3. **Security:** Do you have adequate security to protect against unauthorised access and misuse?

MANAGING CONSENT

Do you have adequate consent to collect, use and disclose health data for this purpose?

It is important that organisations obtain adequate consent to collect, use and disclose health information from an individual. Health information is a subset of 'sensitive information' under the Privacy Act and is treated more strictly than personal information.

Generally, you can collect health information from an individual if:

the individual provides their consent (express or implied); and

the information is reasonably necessary for your activities.

Organisations seeking to collect health information from individuals should ensure that they:

+ understand how they will use the health information, both now and in the foreseeable future;
+ inform the individual of the purpose for which their health information is being collected; and
+ obtain express or implied consent from the individual that their information is being used and disclosed for that purpose.

The Privacy Act distinguishes between the use and disclosure of personal information for "primary purposes" and "secondary purposes".

+ The "primary purpose" is the specific purpose for which the health information was collected. The context in which the health information was collected is relevant to the primary purpose.
+ A "secondary purpose" is any use or disclosure for reasons other than the primary purpose. Where health information is being used for a purpose other than the primary purpose, an individual must provide express consent for their health information to be used in this way to be used in this way (unless consent can be implied or another exception under the Privacy Act applies).

Implied consent can be safely relied upon in some circumstances. For example, where a patient is providing health information to a doctor while receiving a health service from that doctor and the doctor subsequently provides the patient's health information to a specialist the doctor has referred the patient to. In these kinds of situations, the disclosure of the patient's health information is necessarily a part of the service provided by the doctor to the patient.

On the other hand, if the doctor were to disclose the patient's health information to a third-party who is not involved with the provision of the health service, then it is more likely that consent cannot be implied. For example, if the doctor sought to provide a patient's health information to a third party unrelated to the doctor's consultation with the patient, then the doctor should not do so without the express consent of the patient.

If an organisation wishes to change the way it uses an individual's health information and the new use falls outside the scope of consent given at the time of collection (either express or implied), the organisation must seek new consent.

Potential reforms

In the recent DPI Final Report, the ACCC recommended broad reforms to Australia's privacy law (not limited to the digital industry). The ACCC recommended that the Privacy Act be amended to require consent to be "freely given, specific, unambiguous and informed". This suggests the abolition of the concept of "implied" consent. If taken on, these reforms could lead to even stricter requirements for those collecting and using health information.

MANAGING THE DATA SYSTEM

Do you have appropriate data management processes in place?

Organisations should ensure they have appropriate data management processes for collecting, storing, transferring and using health data. Data management systems can include administrative processes, storage or analytics tools and can assist an organisation to exploit the value in their data. Conversely poor systems or processes can hide data value and can also be the source of data mismanagement and breaches.

Recent developments – My Health Records

On 11 November 2019, the Office of the Australian Information Commissioner (**OAIC**) released an annual report of its activities across the digital sector in 2018-19. It received 145 inquiries and 57 complaints about the My Health Record system in 2018-19 and 10 inquiries and 5 complaints about the Healthcare Identifiers Service.

Most of the breaches were attributed to administrative errors, such as intertwined Medicare records where a single record is used interchangeably by two or more individuals, and a number arose from suspected cases of Medicare fraud. It was reported that one breach involved a child incorrectly being given parental authorisation to review a My Health Record.

The OAIC also conducted privacy assessments of regulated entities in the digital sector and opened 3 new assessments of digital health privacy practices - including assessments of private hospitals, pharmacies and pathology and diagnostic imaging services.

OBTAINING CONSENT

One area where data management is important is in the categorisation of distinct types of data. In the health context there are different legal requirements for the handling of health data and personal information. However, these types of information are often collected together. It is important to understand what data fits into each category, and to establish distinct data management processes for each type of data.

Where health data is collected in addition to personal information, additional consents may be required. For example, where an accounts receivable function of a business is being outsourced, it is necessary to determine whether the data being disclosed to the outsourcer contains personal information and/or health data. The outsourcing contract should reflect the legal requirements for the type of data involved (health and/or personal) and the organisation's privacy policy should disclose how it is collecting, using and disclosing each type of data it collects.

A lack of robust data management processes can result in an organisation's privacy practices failing, even though their privacy policies and collection statements say all the right things.

USE AND DISCLOSURE

Where an organisation collects and uses health data for various purposes, or has various business divisions, it will be important for that organisation's data management processes to be capable of recognising and managing these distinctions.

For example, organisations cannot use and disclose health information for a secondary purpose unless it falls within a specific permitted exception such as:

+ the individual would reasonably expect the organisation to use the information for the secondary purpose, and the secondary purpose is directly related to the primary purpose;
+ the use and disclosure is required to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
+ the use and disclosure is in connection with the provision of a health service, research or if the individual is incapable of giving consent (in each case, subject to specific rules); and
+ where required by law or for law enforcement purposes.

Some of these permitted exceptions are irregular in nature – for example, being required to disclose health information for law enforcement purposes. However, for other permitted exceptions that may occur more regularly, an organisation's data management processes should be designed to address these situations – in particular, the exception for secondary purposes directly related to the primary purpose.

Google's Project Nightingale

In November 2019, it was revealed that under a Business Associate Agreement (BAA), Google will have access to Ascension's (a US chain of 2,600 hospitals, doctors' offices and other facilities) patient information. The partnership was referred to as "Project Nightingale". Under the BAA, Google will be using information such as lab results, doctor diagnoses, hospitalisation records, names and dates of birth to develop new software supported by AI and machine learning. Google will also be the designated cloud provider.

It was reported that leaders of the US House Energy and Commerce Committee sent letters to Google and Ascension stating that "...despite the sensitivity of information collected ... reports indicate that employees across Google, including at its parent company Alphabet, have access to, and the ability to download the [patient health information] of Ascension's patients. Concerns have also been justifiably raised about Ascension's decision not to notify its patients that their information would be shared with Google or how their information would be used."

Head of Google Health, Dr David Feinberg issued a media release stating that Google has "strict controls for the limited Google employees who handle such [identifiable patient] data" and that the "Business Associate Agreement with Ascension ensures their patient data cannot be used for any other purpose than for providing our services – this means it's never used for advertising."

DE-IDENTIFICATION AND ANONYMISATION

De-identification of data is one way to protect the privacy of individuals. However, with the increasing capability of technology and the sophistication of cyber-attacks, there is a greater risk that de-identified data can be reversed. In 2016, researchers from the University of Melbourne discovered that they could re-identify a de-identified sample of Pharmaceuticalceutical Benefits Scheme (**PBS**) and Medicare Benefits Scheme (**MBS**) data that was available on data.gov.au, which comprised of health data collected between 1984-2014 for the MBS data and 2003-2014 for the PBS data.

Specific data management processes may also be necessary when individual healthcare identifiers are being collected and used by an organisation. An individual healthcare identifier is a unique 16-digit number that the My Health Record system uses to identify an individual. For example, under the *Healthcare Identifiers Act 2010* (Cth) and *Healthcare Identifiers Regulations 2010* (Cth), healthcare identifiers may only be collected, accessed, used and disclosed for limited purposes. In circumstances where a healthcare identifier is used or disclosed for purposes not permitted by the legislation, criminal and civil penalties may apply.

MANAGING SECURITY

Do you have adequate security to protect against unauthorised access and misuse?

Do we have mandatory IT standards?

In other industry sectors, such as financial services, the industry regulator plays an active role in ensuring minimum IT security standards are met. This can take the form of mandated minimum standards or requiring industry participants to demonstrate their security profile meets certain requirements.

However, there are no mandated IT security standards for handling health data in Australia. Some specific standards have been developed such as:

+ the Information security management in health using ISO / IEC 27002;
+ the National eHealth Security and Access Framework v4.0; and
+ the Australian Government Information Security Manual,

however compliance with these standards is voluntary.

Standards have also been developed specifically for the health sector such as:

+ The OAIC "Guide to health privacy"; and
+ the Australian Digital Health Agency's "Information Security Guide for small healthcare businesses",

however these guidelines are not binding at the general level.

IT service providers who engage with government health agencies will typically be required to meet certain minimum IT security standards (for example, see the Digital Transformation Agency's Secure Cloud Strategy).

HOW DO I MANAGE RISKS WHEN UNLOCKING THE POTENTIAL VALUE OF HEALTH DATA?

Do you have adequate security?

> The **general rule** (under the Privacy Act and the state health records legislation) is that organisations that hold health information must ensure that the information is **protected against loss and unauthorised access, use, modification or disclosure** by taking **such security safeguards** as are **reasonable** in the **circumstances**.

However, the absence of a detailed set of rules or guidelines has meant that the approach across the industry is inconsistent and, in many areas, seriously deficient.

For example, the "Security Check of Australia's Healthcare Information" that was published by the Health Informatics Society of Australia in June 2018 revealed the results of a survey of health industry participants. The results revealed that:

+ about a third of respondents did not have a formal business or governance plan in place for cybersecurity issues;
+ over a third of respondents were either unaware or were certain there were no practices in place to track end user devices and when information is accessed;
+ over 45% of respondents were unsure or not clear at all on how they would respond to a cybersecurity incident; and
+ a quarter of organisations did not do regular business continuity testing.

Unfortunately this has resulted in the health sector ranking highest in terms of where most data breaches occur. In the most recent Notifiable Data Breaches Report for the period between 1 April and 30 June 2019, 19% of data breach notifications occurred in the health sector and 27% of data breaches involved health information.

MANAGING RISK IN M&A TRANSACTIONS

Data is one of the key assets in health M&A and can have significant value implications in an M&A transaction.

Are there privacy risks?

It is critical that the acquisition due diligence focuses on identifying any data privacy risks inherent in the target business and any historic or potential liabilities which could have legal or value implications.

Where data privacy is relevant to the target business, the transaction documentation will typically include robust representations and warranties as to the business' compliance with applicable data privacy regulations (with longer look-back periods than are typical for warranties as to compliance with law). To the extent that specific issues are identified in due diligence, it is not unusual to see specific indemnities in that regard.

Parties to an M&A transaction involving a data-rich business should also take great care in their interactions to ensure that any due diligence, pre-completion access and integration arrangements do not inadvertently contravene any applicable data privacy laws – this can be a delicate process as some categories of personal information may be shared as part of an M&A transaction whilst the sharing of more sensitive information may require consent.

Are there regulatory challenges?

The nature of the data held by the target business may also have implications for the structure that is adopted for an M&A transaction. For example, the transfer or sale of large volumes of data as an asset can often present regulatory challenges.

GOOGLE'S PROPOSED ACQUISITION OF FITBIT

In November 2019, Google announced its proposed acquisition of Fitbit, a health-focused wearables company with products including smartwatches and fitness trackers that track user health metrics from daily step counts to heart-rate, sleep times, BMI and weight. Fitbit have announced that "With Google's resources and global platform, Fitbit will be able to accelerate innovation in the wearables category, scale faster, and make health even more accessible to everyone". While it's still early days, competition regulators have indicated an intention to review the acquisition for any potential privacy and data issues.

Where M&A transactions involve the transfer of large amounts of health data, regulators are likely to look more closely at how competition may be impacted by these transactions, including in novel ways. For example, the German competition authority, the Bundeskartellamt, has started to consider that a company may be considered dominant in a market if it has access to data superior to other companies' data sets. Furthermore, care needs to be taken where the ability to utilise the data is an important objective of the M&A transaction. Depending on the circumstances, an acquirer may find itself restricted in its ability to utilise the target business' data for a different purpose than the primary purpose for which the data was originally collected. This would obviously have significant value implications for the parties as it may, for instance, impact their ability to realise any material synergies that are a driver for the transaction.

Where the acquirer is a foreign person, the Foreign Investment Review Board may also impose conditions, e.g. requiring that certain data not be transferred off-shore.

MANAGING INTERVENTION FROM OTHER REGULATORS

Regulators around the world are increasingly focused on what costs might be being imposed on consumers who are providing personal data in exchange for goods or services.

The ACCC is the national regulator for consumer protection in Australia and has demonstrated a keen interest with respect to data collection and consumers' understanding about these practices during its Digital Platforms Inquiry and Customer Loyalty Schemes Review.

> **"The ACCC is very well placed to deal with a range of future data issues, including in relation to enforcement."**
>
> – ACCC Chair Rod Sims

The ACCC has expressed two main concerns with respect to data practices:

1. **Lack of transparency and consumer control over collection, use and disclosure**

The ACCC is concerned that companies are seeking broad consents from consumers, providing consumers with little insight or control over their data or providing limited ability to opt out.

+ In August 2019, the ACCC commenced proceedings against HealthEngine, Australia's largest online health directory and booking system, for allegedly providing consumer health data to private health insurance brokers for a fee without adequately disclosing this to consumers.
+ In October 2019, the ACCC commenced proceedings against Google for allegedly misleading consumers about the personal location data Google collects, keeps and uses.

2. **Lack of informed and genuine choice for consumers**

The ACCC is concerned that companies make vague disclosures and use unclear or difficult to navigate privacy policies, clickwrap agreements and take-it-or-leave-it terms.

Overseas

Earlier this year, the Bundeskartellamt ordered Facebook to stop collecting user data from third-party websites, finding that Facebook's practices were an abuse of the company's dominant position. Although this decision was subsequently suspended by the Higher Regional Court in Dusseldorf, it demonstrates that data protection is also a priority for overseas regulators.

The action taken by the ACCC and overseas regulators demonstrates a strong willingness to test the boundaries of consumer and competition laws to tackle data practices the regulator perceives as creating consumer harm or distorting the competitive process. With the ongoing digitisation of the health sector, it will be important for companies to find a position where health information can be effectively collected and utilised whilst balancing consumer transparency and protection.

KEY CONTACTS

HEALTHCARE + LIFE SCIENCES LEADS

JOHN LEE
PARTNER,
INTELLECTUAL PROPERTY
T +61 2 9263 4383
E jlee@gtlaw.com.au

SUSAN JONES
SPECIAL COUNSEL,
COMPETITION + REGULATION
T +61 3 8656 3451
E sejones@gtlaw.com.au

OTHER CONTACTS

CHARLES COOREY
PARTNER,
COMPETITION + REGULATION
T +61 2 9263 4019
E ccoorey@gtlaw.com.au

ANDREW HII
PARTNER,
TECHNOLOGY + DIGITAL
T +61 2 9263 4046
E ahii@gtlaw.com.au

KEVIN KO
PARTNER,
CORPORATE ADVISORY
T +61 2 9263 4040
E kko@gtlaw.com.au

CHRIS WILLIAMS
PARTNER,
INTELLECTUAL PROPERTY
T +61 2 9263 4013
E cwilliams@gtlaw.com.au

MICHAEL WILLIAMS
PARTNER,
INTELLECTUAL PROPERTY
T +61 2 9263 4271
E mwilliams@gtlaw.com.au

LUKE WOODWARD
PARTNER,
COMPETITION + REGULATION
T +61 2 9263 4014
E lwoodward@gtlaw.com.au

LIANA WITT
SPECIAL COUNSEL,
COMPETITION + REGULATION
T +61 2 9263 4472
E lwitt@gtlaw.com.au

COURTNEY ROBERTSON
LAWYER,
DISPUTES + INVESTIGATIONS
T +61 2 9263 4360
E crobertson@gtlaw.com.au

The authors would like to thank Dilys Teng, Vanessa Farago-Diener, Sophie Bogard and Meaghan Powell for their contribution to this publication.

GTLAW.COM.AU