Health Legal Report – September 2017

Welcome to the September 2017 edition of the Health Legal Report.

In this issue of the Health Legal Report we discuss:

- ICT Procurement: tips and traps
- Case Note: Duty to Warn of Genetic Risks?
  ABC v St George's Healthcare NHS Trust and Ors [2017] EWCA Civ 336
- Terminating Employees for Misconduct – are your procedures fair?
- Big Data and the Risk of Re-Identification
- Changes to Freedom of Information – Victorian Information Commissioner
- Case Note: Privacy and Health Records
  Seven Network Limited v South Eastern Sydney Local Health District [2017] NSWCATAD 210

We also set out some of the Bills we are tracking throughout Australia, as well as some useful information links.

Level 12, 484 St Kilda Road
Melbourne VIC 3004
ABN 52 104 156 694

Phone: 03 9865 1300
Fax: 03 9012 4353

ICT Procurement: tips and traps

By Sarah Caraher, Senior Associate

Introduction

Good technology is fundamental to your business. There are many ICT products on the market but often they are only as good as the relationships and contracts behind them. Entering into a one-sided supplier contract can significantly diminish your subsequent contractual rights and might leave you without compensation if the product or services fail to deliver. Developing your own suite of templates, or using a government template is always a good starting point as long as the procurement team have been trained in the use of the template.

A complex web of contracts

There are a wide variety of ICT contracts. Some examples are listed below:

- hardware supply and maintenance agreements
- simple licence agreements (for off the shelf or open source software)
- licence and maintenance agreements (where no customisation or configuration is required)
- complex development, licence and maintenance agreements (where customisation or configuration is required)
- software as a service agreements (where software is hosted and accessed via a web browser and involves all customers using the same version of software but with the ability to set configuration options)
- maintenance agreements
- hosting agreements (where the software and client data is being hosted off–site)
- consultancy agreements (such as for website development)
- implementation planning study agreements.

Even within these categories there are many of sub-categories: reseller arrangements, enterprise licenses, pick and mix licenses and single application licenses.

Scope of works

The scope of the ICT works should be clearly articulated at the outset of any major procurement. Important questions include:

- what does the business require now and in the next 5-10 years?
- what model of service is the best fit with your existing infrastructure and service needs?
- what are the high-impact operational risks and how can they best be treated?

If you are not at a point where the scope of the works and deliverables can be sufficiently defined in a contract, then you should consider undertaking an implementation planning study prior to procurement. Leaving a number of key matters, such as deliverables, milestone dates and associated pricing, to subsequent agreement creates significant operational risks. While it may seem innocuous to agree to agree in good faith, such understandings do not create enforceable obligations and are only acceptable where the contract includes a right to terminate the contract early (without penalty) if those matters cannot be agreed. These termination provisions are rarely acceptable to suppliers as they create a high level of commercial uncertainty.

Templates

Depending on the complexity of the proposed arrangement, you can either purpose build a contract or use your own templates or government templates such as the eServices Contract.

If you are using a template it is important to use the current version sourced directly either from your template system or a government website and to cite the version number. Versions used in other procurements, even with the same supplier, may have been amended in a way that is not readily noticeable. To avoid this confusion, it is also prudent to make all amendments in a schedule.

There are usually a significant number of decisions that a template leaves to be negotiated in each contract through the use of an individual order contract or a contract variables document. These decisions range from the specification and scope of works, to system uptime, the status of third party contracts, liability caps, and the treatment of updates and upgrades, to name just a few. Using a template will not avoid the need to negotiate these terms for each contract as they are context specific.

Some common risks in ICT contracts

Some of the common risks in ICT contracting are as follows:

- *Using supplier contracts* – supplier contracts are drafted to protect the supplier and in many instances seek to limit liability to an unacceptably low level.
- *Limitation of liability and liability caps* – template contracts will usually exclude any limitation of liability for damages relating personal injury and property damage as well as breach of third party contracts. However, there will usually be capacity for suppliers to negotiate liability caps for contractual damages and some kind of consequential loss exclusion. Liability caps sought by a supplier should be taken into account in evaluating supplier tender responses. Often pricing will be based on a particular liability position taken in a supplier's contract and therefore it will be difficult to negotiate after the tender is awarded.
- *Consequential loss, loss of use and loss of data* – suppliers often seek to exclude liability for consequential loss, loss of use and loss of data. Recent Australian cases have broadened the test for 'consequential loss' so that it may now include losses that would previously have been considered to be direct losses, such as, liquidated damages for delay. If a consequential loss exclusion is to be negotiated it will be important for you to consider the categories of loss that may arise from a breach and specifically carve out those you do not wish to see excluded, such as loss of data.
- *Security* – with the increasing popularity of 'software as a service' arrangements in which data is hosted off-site, precautions and planned responses addressing issues such as, encryption, back-up and data breach procedures, should be built into the contract. If you are an entity for the purposes of the *Privacy Act 1988*, the new Notifiable Data Breach Scheme (NDB Scheme) will apply from February 2018. Contracts should require compliance with the scheme and a protocol for managing notification.
- *Reseller arrangements* – many maintenance and support contracts will include reference to third party software. The contractor will be a reseller. It is important that the terms of the contract which refer to third parties and sub-contractors are well understood, and that the supplier's obligations are transparent. For instance, are the response times those specified in the RFT and tender response or are they overridden by third party contract terms?

Conclusion

Many ICT contracts are high value and represent a high operational risk to your organisation. Prior to commencing a procurement it is important to have a comprehensive understanding of the current scope and future development of the product and services as well as the key operational risks and the third party arrangements that it may entail. This will allow you to choose the right contract template, request completion of the correct schedules, and enter into negotiations with a well-considered risk tolerance and treatment.

If you have any questions arising out of this article, please contact ***Sarah Caraher*** *on* ***(03) 9865 1334*** *or email* ***sarah.caraher@healthlegal.com.au****.*

CASE NOTE: DUTY TO WARN OF GENETIC RISKS?

ABC v St George's Healthcare NHS Trust and Ors [2017] EWCA Civ 336

By Chris Chosich, Solicitor

Introduction

To what extent does a health service provider owe a duty of care to (third party) relatives of a patient who may be predisposed to a genetic condition?

This is the question raised by ABC against the St George's Healthcare NHS Trust, the South West London and St George's Mental Health NHS Trust and the Sussex Partnership NHS Foundation Trust (**Defendants**). The Defendants learned that ABC's father suffered from Huntington's disease but, consistent with his wishes, did not disclose the diagnosis to ABC. When ABC was subsequently diagnosed with the same condition she sued the Defendants in negligence. The trial judge ordered ABC's statement of claim be struck out on the basis that the Defendants did not owe a duty of care to ABC. However, the Civil Division of the English Court of Appeal quashed that order and remitted the case for trial.

In doing so, the Court has left open the possibility that a duty of care may be owed to third parties with an interest in a patient's genetic information, however whether such a duty exists still needs to be determined at trial.

Facts

In 2007, ABC's father had been found guilty of manslaughter by diminished responsibility and was placed in the care of the South West London and St George's Mental Health NHS Trust pursuant to a hospital order under the *Mental Health Act 1983* (UK). Medical investigations into the reasons for ABC's father's diminished responsibility were conducted at a hospital administered by the St George's Healthcare NHS Trust.

During the course of these investigations, the Defendants formed the view that ABC's father may be suffering from Huntington's disease: a hereditary, incurable and fatal disease that is associated with disruptions of movement, cognition and behaviour. A person with Huntington's disease has a 50% chance of passing the condition on to their children.

Genetic testing confirmed the diagnosis of Huntington's disease. Subsequently, the father's medical team considered whether ABC should be informed because the possible implications meant that she may have had 'a right to know'. The father, who was involved in these discussions, said he did not want ABC to know in order to protect her from distress. On the same day as these discussions, ABC informed her father that she was pregnant. Her father maintained that ABC should not be informed and ABC gave birth in early 2010.

As it transpired, ABC was accidentally informed of her father's diagnosis by one of her father's doctors a few months after giving birth. ABC underwent genetic testing, which showed that she suffered from Huntington's disease. When the case was filed, it was too early to conduct tests to determine if ABC's daughter also had the condition.

Procedural history

ABC sued the Defendants in negligence. She argued that the defendants owed her a duty of care that required them to act reasonably when considering whether they should have disclosed her father's diagnosis of Huntington's disease. As a consequence, she continued, she had suffered psychological harm and lost the opportunity to

consider terminating her pregnancy (either because of the risks that the child would have the disease, or because she did not want to have a child in the knowledge that she, ABC, would become seriously disabled in later life).

The Defendants argued that they did not owe ABC a duty of care and that a duty of care should not be imposed. As such, they applied for ABC's claim to be struck out. The trial judge, Nicol J, granted the application.

ABC then appealed to the English Court of Appeal, Civil Division.

Issues

The issue on appeal was whether Nicol J had been right to strike out ABC's claim. The question was not whether the duty of care contended for by ABC existed, but only whether or not it was arguable that such a duty could exist. Thus, the appeal only concerned whether a court would consider the existence of the proposed duty of care.

Because the duty of care contended for by ABC was novel, she had to show it was arguable that the kind of relationship between her and the Defendants satisfied the three elements set out *in Caparo Industries Plc v Dickman* [1990] 2 AC 605:

1. the relationship was one in which harm was foreseeable;
2. the relationship can be characterised as one of proximity; and
3. it is fair, just and reasonable to impose a duty on one party for the benefit of the other.

For the purposes of the argument, the Defendants accepted that the first two elements existed. The case turned upon whether imposition of a duty of care between ABC and the Defendants was fair, just and reasonable.

ABC's argument

ABC argued that it was fair, just and reasonable to impose a duty of care on the Defendants for her benefit because she had a 'special relationship' with the Defendants. This relationship arose, said ABC, either because the Defendants knew important information about ABC (i.e. the risk of a genetic condition) that had a direct effect on her 'health, welfare and life', or because the Defendants provided her with family therapy associated with her mother's death and had a responsibility for therapeutically addressing the relationship between ABC and her father.

Cognisant that the Defendants would argue that the alleged duty of care would conflict with their obligations of confidence to her father (and would thus be unfair, unjust or unreasonable to impose), ABC relied upon professional guidance to argue that the duty of confidentiality was not absolute.

In particular, she pointed to the Royal College of Physicians', the Royal College of Pathologists' and the British Society of Human Genetics' *Consent and Confidentiality in Genetic Practice, Guidance on Genetic Testing and Sharing Genetic Information*, which stated:

> In special circumstances it may be justified to break confidence where the aversion of harm by the disclosure substantially outweighs the patient's claim to confidentiality. Examples may include **a person declining to inform relatives of a genetic risk of which they may be unaware, or to allow the release of information to allow specific genetic testing to be undertaken**. (emphasis added)

Similarly, General Medical Council's Good Medical Practice guidance stated that:

> If a patient's refusal to consent to disclosure leaves others exposed to a risk so serious that it outweighs the patient's and the public interest in maintaining confidentiality, or if it is not practicable or safe to seek the patient's consent, you should disclose information promptly to an appropriate person or authority. You should inform the patient before disclosing the information, if practicable and safe, even if you intend to disclose without their consent.

In light of this guidance, ABC argued that there are professional (as opposed to legal) obligations that would require disclosure to those who, while not in a doctor-patient relationship with the relevant medical practitioner, have an interest in that information (such as the diagnosis of Huntington's disease). As such, this argument continued, it would not be unfair or unreasonable to impose a duty of care to the same effect.

The Defendants' argument

In response the Defendants argued that various policy reasons pointed against the imposition of a duty of care. In particular, they alleged that imposition of the duty of care contended for by ABC

would conflict with the duties already owed by doctors to their patients (such as the duty of confidentiality). Further, they continued, the prospect of disclosure (even if only theoretical) would undermine confidence in the doctor-patient relationship because patients could not be certain their information would remain confidential. The Defendants concluded that these features would render the duty unworkable, either because doctors would not know if they should disclose information that may be unwanted by a third party or because the duties to the patient and interested third party would be difficult to resolve. As a consequence it would be unfair, unjust or unreasonable to impose the duty.

Decision

Lord Justice Irwin (with whom Lady Justice Gloster and Lord Justice Underhill agreed) held that it was at least arguable that the duty of care contended for by ABC existed. As such, the Court quashed the order striking out ABC's claim and remitted the case for trial.

Given the nature of the question on appeal (whether it was *arguable* that a duty of care existed) Irwin LJ did not conclude on the merits of each argument. Instead, his Honour only considered whether, with reference to the countervailing reasons raised by the Defendants, the existence of duty was arguable.

Public interest in disclosure?

His Honour started by observing that there was, as recognised in the professional guidance adduced by ABC, arguably a public interest in disclosures of some kinds of patient information to third parties. The imposition of a duty to that end would likely improve public confidence in the medical profession by holding them to the guidance and could be consistent with the trend towards individual autonomy in the field of medical negligence.

The latter argument requires some expansion. Lord Justice Irwin noted that the legal trend in negligence has been towards facilitating *patient* autonomy by empowering those patients to make decisions about their treatment. However, Irwin LJ continued, it is potentially inconsistent to emphasise the autonomy of an individual patient above the autonomy of specific third parties known to the doctor who would become patients if the doctor disclosed information in which those third parties had an interest. Lord Justice Irwin accepted that it could be argued that the interest of third parties could give rise to a public interest in disclosure. In particular, Irwin LJ said:

> [ABC] argues that there is a public interest in preventing the unwitting conception or birth of a child who may need significant state support because of the parent's potential inability to bring up her child, and where that child itself has such a high chance of growing up only to succumb herself to such a fell disease. … I cannot conclude that the Claimant's position is unarguable.

Conflict of duties?

Turning to the issue of a conflict of duties between the interests of patients and third parties, Irwin LJ accepted that the imposition of the duty contended for by ABC would lead to some difficulties for medical practitioners. His Honour observed that the difficulty already existed (as evidenced by the need for clinical guidance on the matter) and approved of ABC's argument that a legal duty could encourage the protection of the interests of patients and third parties by ensuring that practitioners carry out an appropriate balancing exercise when considering whether to disclose patient information to a third party without a patient's consent.

While accepting that the prospect (even a theoretical one) of involuntary disclosure of patient information by a doctor could undermine trust within the doctor-patient relationship, Irwin LJ went on to observe that this was not necessarily a reason to avoid imposing a duty of care because the imposition of a duty of care would not automatically entail legal liability, nor would it always require disclosure of information. Rather, such a duty would only require a medical practitioner to act reasonably, as informed by peer opinion and professional standards. Thus, Irwin LJ observed:

> Common law liability would be measured against those standards, with the relevant professional practice and guidance very much to the fore. Indeed it seems to me evident, given the difficulty of such decisions, that the Courts would allow considerable latitude to clinicians faced with such a dilemma. Once again in relation to this policy reason, I reach no decided conclusion save that the matter is to my mind clearly arguable.

Floodgates?

A key concern with the imposition of any new duty of care is the potential to "open the floodgates" to a raft

of similar, but slightly different, claims. The Defendants argued that medical practitioners will hold large amounts of information that may be relevant to third parties – such as information about sexually transmitted diseases, highly contagious diseases and terminal illnesses – in which third parties (such as sexual partners and family members) may have an interest.

However, Irwin LJ did not perceive any difficulty in defining the bounds of ABC's proposed duty of care:

> it seems to me this policy reason lacks any bite when applied to geneticists. As will already be clear from the professional guidance to which I have referred, and indeed from the inherent nature of genetic medicine, geneticists frequently acquire definite, reliable and critical facts of clinical significance about their patients' relatives.

The reliability of the information and its importance to interested family members who would become patients if that information were disclosed meant that, in Irwin LJ's opinion, the case of genetic information is distinguishable from the other scenarios raised by the Defendants.

Judicial restraint?

Finally, Irwin LJ dealt with the question of whether imposition of the alleged duty of care would be inconsistent with the incremental and cautious development of the law. His Honour held that it was not because of American authorities (*Tarasoff v Regents of the University of California* (1976) 551 P.2d 334 and Safer v Pack 291 N.J.Sup. 619, 677 A. 2d 1188) in which courts recognised a duty to disclose or warn an interested third party about risks of serious physical harm (in Tarasoff) or a genetic predisposition to metastatic bowel cancer (in Safer), in spite of the obligations of confidence owed by health practitioners.

Having found that ABC's claim was arguable, the Court reinstated ABC's claim and remitted the matter for trial.

Australian relevance

ABC's claim is now free to progress to trial. It will be a matter for the courts to determine whether a duty of care to disclose genetic information to interested third parties exists. Given the difficult questions of law and policy to be answered, there is a strong prospect that the case will go on appeal from trial.

This case raises the question about whether a similar duty of care could be recognised in Australia. At the outset it is important to note that an Australian court applies a different test to determine the existence of a duty of care. Rather than the three step test used by English courts, the High Court of Australia has made it clear that Australian courts must consider all the 'salient features' of a case when deciding whether or not to impose a duty of care, including the existence of other duties and obligations. Thus, the existence of State and Federal privacy legislation will be one consideration determining the existence (if any) of a duty of care owed to a patient's genetic relatives. Given the fragmented nature of privacy regulation in Australia, courts would need to grapple with the possible implications of recognising a duty that could possibly conflict with those protections. Further complicating the assessment is that the applicable privacy framework differs from jurisdiction to jurisdiction, and on the private or public nature of the health service provider.

At a Federal level, the *Privacy Act 1988* (Cth) allows **private-sector organisations** to disclose a patient's genetic information without consent in order to lessen or prevent a serious threat to a genetic relative of the patient provided that the disclosure is made to the relative and is made in accordance with Guidelines made under section 95AA of the *Privacy Act 1988* (Cth) (which require medical practitioners to consider certain matters, to discuss disclosure with other health practitioners and to document the process leading to disclosure). Though in some jurisdictions, such as Victoria, private sector organisations will also be subject to State-based privacy legislation.

For public sector organisations, only the relevant state-based privacy protections will apply to genetic information. However, the existence and scope of these protections differ from jurisdiction to jurisdiction. Some jurisdictions, for example, do not expressly address genetic information, others define genetic information as health information (which may usually only be disclosed without consent in extenuating circumstances, such as where there is a serious and imminent threat to a third party's life, health or wellbeing) while New South Wales has moved to mirror the Federal protection.

Given the increasing prevalence and utility of genetic information in health-care settings, it may only be a matter of time until a similar case is brought in Australia. It will be interesting to see how a court would deal with the intersection between a duty of care owed to third parties, and the (patchwork) privacy protections that limit the disclosure and sharing of health (and particularly genetic) information.

*If you have any questions arising out of this article, please contact Chris Chosich on **(03) 9865 1329** or email **chris.chosich@healthlegal.com.au**.*

Compliance Alert Service

In response to client demand we have developed a compliance alert service which complements our existing legislative compliance products and services.

Updates to the Compliance Register and Self-Assessment Questions are delivered on a quarterly in arrears basis so that you are updated on legislative changes which have occurred in previous 3 month period.

We have now launched an alert service which provides you with pro-active advanced warning of the commencement of new significant Acts. "Significant" Acts means those which will have a significant operational impact on your organisation. As part of this alert, we will provide you with a summary of the legislation and provide you with a link to the relevant Act.

This alert service will allow you to prepare for new legislation before the Acts have commenced.

LAW COMPLIANCE

If you would like to add this service to your current subscription (or if you have any questions), please contact ***Teresa Racovalis*** *on* ***(03) 9865 1337*** *or* ***teresa.racovalis@lawcompliance.com.au***.

Policy Service

As a result of client demand we have extended our compliance services to cover policy wordings.

From our perspective:

- understanding where a legislative obligation fits within a policy framework can be difficult, and
- organisations often don't have sufficient resources to keep their policies legally up to date.

Our new service aims to assist organisations to overcome these issues.

Health Legal now offers a new quarterly update service where subscribers are given:

- guidance about the types of policies that may be affected by a legislative change,
- suggested wording for relevant policies to allow subscribers to modify their own policies, and
- completely new policies if Acts in new areas of law are introduced (or existing Acts are substantially re-written).

*If you have any questions about the Policy Service please contact **Teresa Racovalis** on **(03) 9865 1337** or **teresa.racovalis@lawcompliance.com.au**.*

Terminating Employees for Misconduct – are your procedures fair?

By Alon Januszewicz, Associate Legal Counsel

Introduction

Employers will be familiar with the concept of procedural fairness (also referred to as natural justice) and the need to ensure that employees are subjected to a process which complies with its requirements. At its core, procedural fairness requires that:

- the employee is afforded the opportunity to respond to the allegations, and
- the decision maker is unbiased.

While these concepts appear clear and intuitive, the Fair Work Commission (FWC) routinely finds that employers have not complied with these principles with the result that the dismissal may be found to be unfair. In particular, the risk of falling short of these requirements can arise where an employer considers the employee's misconduct to be so obvious, and the evidence overwhelmingly clear, with the result that the decision to dismiss the employee is made in haste and without affording the employee a full opportunity to respond to the allegations. In this article, we report on recent cases which focus on the first limb of procedural fairness and the lessons which can be learned from the FWC's commentary on the process followed by employers.

Insufficient time to respond

In *Webb v The Trustee for SWC Unit Trust T/A Salisbury Day Surgery* [2017] FWC 2572, Ms Webb applied for an unfair dismissal remedy after having been dismissed due to alleged dishonest conduct in submitting inaccurate time sheets and also due to bullying behaviours.

The letter of allegations sent to Ms Webb invited her to respond to the employer's allegations that she had engaged in bullying, fraud and theft. The evidence relied upon by the employer to substantiate the allegations included building access records which apparently were inconsistent with the hours claimed by the employee. Ms Webb provided a written response, however, she was summarily dismissed.

Was the dismissal (procedurally) unfair?

Ms Webb submitted that there were serious procedural defects with the dismissal process. The defects included being provided with less than 48 hours to respond to the alleged incidents (some of which dated back 18 months) and not being provided with the records relied upon by the employer in making the decision to terminate her employment.

The FWC's consideration – The Small Business Fair Dismissal Code

The employer was a small business for the purposes of the Fair Work Act (employing under 15 employees). Accordingly, the FWC was required to satisfy itself that the dismissal was not inconsistent with the Small Business Fair Dismissal Code (the Code).

The Code relevantly provides that:

> …It is fair for an employer to dismiss an employee without notice or warning when the employee believes on reasonable grounds that the employee's conduct is sufficiently serious to justify immediate dismissal. Serious misconduct includes theft, fraud, violence and serious breaches of occupational health and safety procedures…

The employer submitted that Ms Webb's immediate dismissal was consistent with the Code because she had engaged in conduct that amounted to fraud and theft.

The FWC held that it was not established, on the evidence, that the conduct of the employee was dishonest, only that on the employer's evidence there was a discrepancy in the time sheets

submitted. On the basis of the above, the FWC found the dismissal to be inconsistent with the Code.

Was the Employee given an opportunity to respond to the allegations?

The time sheets in question covered a period of 18 months. In that context, the FWC held that it was 'entirely unreasonable for the [employer] to expect the [employee] to provide a cogent response to such a range of allegations … in less than 48 hours.'

The FWC also remarked that the process was deficient in that the employer 'did not put the full records, or the reasons for the dismissal, in their completeness, to the [employee] before her dismissal. The [employer] erred by not affording her a reasonable period to respond to and to consider the allegations in a proximate way to the dates of alleged conduct'.

Taking into account the factors above, the FWC found that the Applicant had been unfairly dismissed. The FWC did not, however, order the payment of any compensation in this instance because it was ultimately satisfied that there was a valid reason for the dismissal (even if the employee was not found to have been dishonest).

Failure to provide the employee with the evidence in support of the allegations

In *Tavassoli v Bupa Aged Care Mosman* [2017] FWC 3200, the employee was covertly filmed by a colleague. Bupa alleged that Ms Tavassoli (who was employed as an 'Assistant in Nursing') laughed at the fact that two residents had passed away during the shift of a colleague. Another video allegedly showed that Ms Tavassoli ignored the buzzers of residents. After being escorted from Bupa's premises and being told that she needed to have a discussion with management, but before any allegations were put to her, Ms Tavassoli decided to resign. Later Ms Tavassoli decided to retract her resignation, and the FWC held that Bupa's refusal to allow her to do so was procedurally unfair.

The Commissioner stated:

> I struggle to see how the principles of procedural fairness can be satisfied by the actions of Bupa. Employees have a right to know the case that they have to answer. Bupa had an obligation to show Ms Tavassoli the video footage, particularly when it forms the sole foundation of the allegations. Simply making generalised accusations when specific information was available is a form of entrapment. The decision to terminate an employee should not be based on a memory test but rather the employee's considered response to specific accusations.

In this case, Ms Tavassoli was not afforded procedural fairness because she was not shown the videos on which the allegations were based. A procedurally fair process would have, at the least, required that the employee be provided with the allegations as well as the evidence in support of the allegations. In this case, given the employee's decision to resign, the employer ought to have allowed Ms Tavassoli to rescind her resignation while the investigation was completed.

Investigating alleged misconduct

The investigation, and the subsequent disciplinary actions, must be procedurally fair even in the face of very serious allegations and overwhelming evidence.

The circumstances of each investigation will be different, however, the above cases highlight some principles which must be complied with: the employee must be provided with complete information about the allegations, ideally the information should be provided as soon as practicable after the conduct and a reasonable period should be allowed for the employee to consider and respond to the allegations.

It is important to have policies and procedures that reflect the requirements of procedural fairness. However, these documents are only a starting point and it is in the implementation of those policies that the risks lie.

The employer's personnel must remain objective and ensure that the steps taken in the investigation and subsequent disciplinary action are reasonable, defensible and comply with the rules of procedural fairness. Although these procedural steps may appear relatively trivial in the face of very clear evidence demonstrating the employee's misconduct, failure to comply with these procedural requirements can undermine the employer's decision to dismiss or discipline the employee.

*If you have any questions arising out of this article, please contact Alon Januszewicz on **(03) 9865 1312** or email **alon.januszewicz@healthlegal.com.au**.*

Big Data and the Risk of Re-Identification

By Chris Chosich, Solicitor

Introduction

On 12 September 2016, researchers at the University of Melbourne alerted the Commonwealth Government that it was possible to re-identify ostensibly "de-identified" Medicare Benefits Scheme (MBS) data that had been released for public access and analysis. The MBS Re-identification Event attracted significant media attention, generated an Australian Office of the Information Commissioner (OAIC) investigation and resulted in the introduction of the Privacy Amendment (Re-identification Offence) Bill 2016 (Cth).

The MBS Re-identification Event is a reminder of the importance of considering the privacy implications of big data analytics.

Big data

Big data refers to the advanced capacity to collect, store, handle and analyse data in ever increasing quantities. A common definition is Gartner's "three Vs":

> …high-**volume**, high-**velocity** and/or high-**variety** information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization.

Put simply, the difference between data and *big* data is one of scale. More data, with more data fields, allow greater insights and observations to be drawn in ways that older datasets could not offer.

Big data in the health sector

Huge amounts of health sector data are already collected for the purposes of administering the complex systems that underpin the provision of health services in Australia.

At a Federal level, the administration of the MBS, Pharmaceutical Benefits Scheme (**PBS**) and (to a certain extent) the My Health Record system create rich datasets that, when processed, could shed light on emerging trends in the sector, assist in improving system efficiency and inform research. Indeed, the potential of these datasets has recently been recognised by the Productivity Commission, which noted that health care data could be used to inform policy decisions, gain a clearer understanding of patient experience and detect positive and negative trends at an early stage.

Public and private health service providers will also collect their own potentially useful datasets. Even smaller organisations, with their correspondingly small datasets, can benefit from big data analytics by creating partnerships with other organisations in order to pool useful information.

However, the public utility of these datasets butts up against the private interests of individuals in maintaining their privacy. The challenge for health service providers is how to benefit from big data while simultaneously protecting sensitive and identifying information.

De-identification: Protecting information

The *Privacy Act 1988* (Cth) (which applies to private sector organisations) protects information that reasonably identifies an individual. Similar legislation applies to public sector organisations at State and Territory levels and (in some cases) to organisations handling identifying health information. While these Acts require organisations to handle identifying information in specific ways, they do not generally apply to information that has been de-identified.

This begs the question, when is data de-identified? In short, personal information is 'de-identified' where it is no longer about an identifiable or reasonably identifiable individual (see section 6(1) of the *Privacy Act 1988* (Cth)). Typically this will require, at the very

least, the removal of names, addresses and contact details. However, even with this information removed, datasets can theoretically (depending on their source) be reasonably identifiable through the application of specialised knowledge, or connection with other datasets. Thus, it is sometimes necessary to apply cryptographic techniques in order to truly de-identify the information. Such techniques include:

- removing unique identifiers (e.g. income, profession) that may, either by themselves or in combination with other information, identify a particular person;
- aggregating information into ranges (e.g. data expressed as being that of people 25-30 years old);
- swapping identifying information between individuals in order to maintain the integrity of the information as a whole, but confound attempts to identify a particular person;
- generating synthetic data with similar patterns to the original dataset, but without identifying features; and
- suppressing data that may aid in identifying individuals.

The challenge posed by big data is whether big data can be sufficiently de-identified while retaining the data's integrity for analysis. As the MBS Re-identification Event shows, it is possible for sufficiently skilled and motivated people to decrypt ostensibly de-identified data (**cryptographic attacks**), or to re-identify the data by comparison with other (identifying) datasets (**linkage attacks**). It was the former kind of re-identification that occurred in the MBS Re-identification Event.

MBS Re-identification Event

The MBS Dataset was a 10% slice of MBS information released by the Commonwealth Government on its new 'data.gov.au' website (which allows the Commonwealth Government to share datasets with the public). The dataset contained (ostensibly de-identified) information about services provided by MBS item, the location of service provision and, importantly, the encrypted healthcare provider and recipient numbers for each MBS funded service.

With the release of this potentially sensitive dataset, University of Melbourne researchers decided to test its security against re-identification. Using only publically available information about the encryption mechanisms used by the Commonwealth, the researchers were able to decrypt every service provider identifier in the MBS dataset, thereby allowing the individual health practitioners to be identified. In theory, patient identifiers could have been decrypted but the researchers did not do so.

On becoming aware that the MBS Dataset had been re-identified, the Government removed the MBS dataset and a similar PBS dataset from the 'data.gov.au' website. An OAIC investigation into the matter is pending. However, the Government has not waited for the results of this investigation and has moved swiftly to introduce legislative changes to protect Commonwealth datasets.

The Privacy Amendment (Re-identification Offence) Bill 2016 (Cth)

On 12 October 2016, the Federal Attorney-General introduced the *Privacy Amendment (Re-identification Offence) Bill 2016* (Cth) (**Bill**) into the Senate. The Attorney-General's second reading speech explains that the purpose of the Bill is:

> to ensure that the considerable benefits associated with the release of public sector datasets can be realised whilst upholding the highest standard of information security and protecting the privacy of Australians.

To this end, the Bill would amend *the Privacy Act 1988* (Cth) to make it an offence for an entity (which includes individuals, body corporates, small businesses and Commonwealth agencies) to: (1) intentionally re-identify information that has been disclosed by a Commonwealth agency; and (2) to intentionally disclose that re-identified information. Importantly, the offences will not apply in respect of datasets made available by State and Territory agencies (which are regulated by other privacy laws).

Criminal penalties of up to 2 years imprisonment and/or a fine of $21,600 would apply to a contravention of the Bill, while civil penalties extend to fines of up to $108,000.

There would be some exemptions from the Bill's provisions, including for entities providing services under contract to the Commonwealth, for acts

undertaken under an agreement with a Commonwealth agency and for entities exempted by the Attorney-General. Further, State and Territory authorities (such as universities and health services) would not be subject to the proposed re-identification offences (though their employees may be liable in their individual capacities).

Effect on research

Somewhat controversially, the Bill's proposed offences will apply to individuals acting in their personal capacity. Individuals have not typically been required to comply with the Australian Privacy Principles (except in some limited circumstances) and some, such as the University of Melbourne cryptographers who were responsible for the MBS Re-identification Event, are concerned that the Bill will chill legitimate research into cryptography while doing little to address re-identification for criminal or fraudulent purposes.

Whether a researcher would be exempt from the proposed offences depends on whether they operate in the public or private sector, and the scope of their duties of employment. Public sector researchers engaged by a State or Territory authority (such as a university or a health service) could rely on an exemption if they are acting within their duties of employment (see proposed s 16CA(2) of the Bill). However, if these employees acted outside their duties of employment, they would fall foul of the re-identification offences. Private sector researchers would not be exempt from the Bill, however the Attorney-General has indicated that the Government would consider implementing an appropriate exemption if it were in the public interest.

In response to concerns about the status of researchers (and other matters), a Senate Committee recently considered the Bill and recommended that it be passed, in part because researchers are often public sector employees and will thus be exempt from the re-identification offences. In any event, the Bill remains before the Senate, and is yet to be considered by the House of Representatives.

Protecting personal information

Big data has big potential and correspondingly big risks. The MBS Re-Identification Event makes it clear that effective de-identification of data is vital to ensure the benefits are balanced against the risks to personal privacy. In particular, decisions to publish de-identified datasets should be made with consideration of the integrity of techniques used to de-identify data in balancing the benefits and risks of big data.

The MBS Re-identification Event also reminds organisations that handle information to consider privacy as an integral part of data management, especially where that data is to be shared publically or privately. One key question that may be useful to ask is what the OAIC calls the 'motivated intruder test'. It asks:

> whether a reasonably competent motivated person with no specialist skills would be able to identify the data or information (the specific motivation of the intruder is not relevant). It assumes that the motivated intruder would have access to resources such as the internet and all public documents, and would make reasonable enquiries to gain more information.

The answer in the MBS Re-identification Event was a resounding yes.

For Commonwealth agencies, the Bill will (if it is passed) provide legal protections that supplement technical and systemic protections by imposing criminal sanctions for re-identification of de-identified Commonwealth datasets. However, given that the efficacy of such laws will necessarily depend on effective detection and enforcement, the Bill only forms a piece of the data protection puzzle and the efficacy of de-identification techniques will still be of central importance.

For private sector and State and Territory entities, appropriate de-identification techniques and strong privacy systems are of even greater importance because those entities will not have the added legal protections proposed by the Bill.

Finally, the MBS Re-identification Event reinforces the importance of privacy by design, and reminds all organisations of the reputational (and potentially financial) risks of unintentional public releases, or of re-identification events.

*If you have any questions arising out of this article, please contact Chris Chosich on **(03) 9865 1329** or email **chris.chosich@healthlegal.com.au**.*

Changes to Freedom of Information – Victorian Information Commissioner

By Claudia Hirst, Legal Counsel

Introduction – Summary of changes

The *Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017* (Vic) has amended the *Freedom of Information Act 1982* (Vic) (the FOI Act) making significant changes to the way in which Freedom of Information (FOI) matters are dealt with in Victoria. The FOI act is amended effective 1 September 2017.

Victorian Information Commissioner

A key change is the establishment of the Office of the Victorian Information Commissioner (**OVIC**), and the abolition of both the Freedom of Information Commissioner (**FOI Commissioner**) and the Commissioner for Privacy and Data Collection (**PDC Commissioner**). The head of the new OVIC is the Information Commissioner (**IC**) who has the same powers and functions held by the FOI Commissioner and the PDC Commissioner. Mr Sven Bluemmel has been appointed as the IC. Deputy Commissioners have not yet been appointed.

Enforceable Professional Standards and OVIC investigations

The Act empowers the IC to set professional standards providing clear guidance on how the Act should be administered. These professional standards are binding on agencies and principal officers. Non-compliance with the professional guidelines may form the basis of a complaint to the IC.

The IC also has power to initiate an own motion review of the performance by agencies of their functions under the Act.

Time limits

Previously, section 21 of the FOI Act required an agency to take all reasonable steps to notify an applicant of a decision on a request as soon as practicable, and no later than 45 days after the request was received. Now, section 21 requires an applicant to be notified of a decision not later than 30 days after the day on which the request was received by the agency.

The 30 day rule can be extended by 15 days if consultation is required as prescribed by various exemptions and also by 30 days with agreement with the applicant. The 30 day extension may be repeated any number of times but an extension cannot be made after the time limit for a notice of decision has expired.

Agencies should note that the deemed refusal provisions of s 53 remain unchanged so that failure to provide a decision within the time period may result in a direct review application to VCAT rather than to the IC.

The Act has also reduced the time for an agency to lodge an application to VCAT seeking a review of OVIC decisions from 60 days to 14 days.

Consultation and exemptions to the requirement

The following sections dealing with exempt documents have been amended to introduce mandatory consultation with and notification of affected persons. These sections are: s 29, s 29A, s 31, s 31A, s 33, s 34 and s 35. Section 33 relates to documents affecting personal privacy. Previously, this section required an agency to advise a person if the agency had decided to grant access to a document containing the personal affairs of that person and to notify them of their right to appeal. The FOI Act now adds the requirement to consult the person prior to making the decision and to seek their view as to whether they consent to the disclosure.

Section 34, documents relating to trade secrets, previously did require consultation with an undertaking to seek their views on whether the disclosure would expose them unreasonably to disadvantage and this requirement is maintained in the Act. However, a further section is added to allow for the provision of consent.

Similar consultation requirements have also been added to s 35, documents provided in confidence.

If the person does consent to the disclosure under sections 33, 34 or 35, they are prohibited from seeking a review of that decision at a later date. The requirements to notify of a decision remain in place, unless, of course, the person has consented to the disclosure.

Each of s 33 and s 35 make provision for removing the consultation requirement if: consultation would endanger life or physical safety, cause undue distress, be unreasonable in the circumstances; or be otherwise impracticable.

Powers to compel further search

It is also important to note that the Act has introduced section 49KA, which applies if the IC reasonably believes that an agency has failed to undertake an adequate search for documents related to a decision under review. During the review, the IC may give a notice to the agency to require the agency:

- in the case of a decision of an agency under section 25A of the Act, to process or identify a reasonable sample of the documents to which the request relates; or
- in any other case, to further search or to cause a further search to be undertaken for documents in the possession, custody or control of the agency.

The agency must comply with the IC's requirement within the reasonable period stated in the notice, being not less than 10 business days.

New IBAC exemption

The Act also introduces a further exemption at section 31A relating to documents associated with an investigation by or notification to the Independent Broad-based Anti-corruption Commission (IBAC).

Procedural considerations

Organisations should update their FOI policies and procedures to comply with the amended legislation.

*If you have any questions arising out of this article, please contact **Claudia Hirst** on **(03) 9865 1340** or email **Claudia.hirst@healthlegal.com.au**.*

Precedents/Standard Form Agreements and Policies

Due to client demand, we have developed a range of standard form Agreements and Policies which are commonly used by health, aged care and community service providers. The documents have been prepared in a template form so they can be completed by your staff and include service contracts for the provision of pathology and radiology services, requests for tenders, leases and supply of goods contracts.

Precedents recently added to our range include a consultancy suite hire contract, supply of equipment with associated services agreement, sponsorship agreement and a short form Request for Proposal.

*For further information about these precedents please contact **Natalie Franks** on **(03) 9865 1324** or **natalie.franks@healthlegal.com.au**.*

CASE NOTE: PRIVACY AND HEALTH RECORDS

Seven Network Limited v South Eastern Sydney Local Health District [2017] NSWCATAD 210

By Giovanni Marino, Senior Solicitor

Introduction

The New South Wales Civil and Administrative Tribunal (**Tribunal**) found that certain hospital CCTV footage could be released under freedom of information legislation, despite public interest and privacy concerns, if the faces, heads, necks and any tattoos or other identifying marks of persons in the footage were pixelated.

Facts

The CCTV footage in question was collected by two hospitals that form part of the South Eastern Sydney Local Health District (**LHD**).

In March 2016, a television broadcaster, Seven Network, made a request to access the LHD's 'incident reports and video of assaults on security and staff at hospitals since July 1, 2014'. The request was made under the applicable New South Wales freedom of information legislation, the *Government Information (Public Access) Act 2009* (NSW) (**GIPA Act**).

Section 9 of the GIPA Act provides that a person who applies for access to government information (the LHD information in this case) has a legally enforceable right to be provided with access unless there is an overriding public interest against disclosure of the information.

The LHD provided Seven Network with the requested incident reports, but determined that the CCTV footage could not be produced.

There were three relevant pieces of footage, described as follows:

- **Footage 1:** An incident in the 'Safe Assessment Room' (SAR) of 'Hospital A', which showed a male patient and a doctor conversing, and then the patient attempting to kick the doctor, following which the patient is subdued by other staff. (SARs were described as separate, secure rooms in the Emergency Department that provide private spaces to manage a number of sensitive needs, such as grieving relatives, to allow high-level observation of patients, and to undertake assessment and treatment of patients attending for mental health services.)
- **Footage 2:** A man, likely to be a patient, approaching the entrance to the Emergency Department of 'Hospital A'. The man is approached by a security guard, and attempts to strike the guard. The man is restrained by security staff until police arrive. Nurses and members of the public can also be seen.
- **Footage 3:** A young man attempts to strike a security guard outside the Emergency Department at 'Hospital B'. Two other members of the public are also visible along with other security guards. The security guards restrain the young man and take him inside the Emergency Department.

In June 2016, Seven Network applied to the New South Wales Information and Privacy Commissioner for a review of the LHD's decision. The Commissioner recommended that the LHD make a new decision and consider whether it could redact information from the footage through pixelation, or create a new record by removing sections of the footage.

In September 2016, the LHD refused Seven Network access to the footage, on the basis that there was an overriding public interest against disclosure of the

footage, as it contained sensitive health and personal information, and there was no ability of the LHD to redact or pixelate the information.

Seven Network applied to the Tribunal for review of this decision.

Consideration by the Tribunal

The Tribunal considered the relevant provisions of the GIPA Act, including:

- Section 12, which relevantly provides that there is a general public interest in favour of disclosure of government information.
- Section 13, which relevantly provides that there is an overriding public interest against disclosure of government information if there are public interest considerations against disclosure and, on balance, those considerations outweigh the public interest considerations in favour of disclosure.

Factors in favour of disclosure (as noted in section 12 of the GIPA Act) included:

- Disclosure of the information could reasonably be expected to promote open discussion of public affairs, enhance government accountability or contribute to positive and informed debate on issues of public importance.
- Disclosure of the information could reasonably be expected to inform the public about the operations of agencies and, in particular, their policies and practices for dealing with members of the public.

Seven Network submitted that it intended to broadcast the footage as a news item to increase public awareness of violence towards hospital staff, and to stimulate 'debate regarding the appropriate legislative and law enforcement response', which was consistent with the factors in favour of disclosure above.

As part of its evidence, Seven Network also offered to pixelate the CCTV footage at its own cost, either by undertaking the task itself, or by paying a third party retained by the LHD to do so.

The LHD relied on certain factors against disclosure as are set out in section 14 of the GIPA Act. These factors included:

- Disclosure of the information could reasonably be expected to reveal a person's personal information and health information (in breach of privacy and health records legislation).
- Disclosure of the information could reasonably be expected to expose the LHD staff and patients to a risk of harm, serious harassment or serious intimidation. The LHD submitted that publication of the footage put hospital staff, including doctors, nurses and security officers, at risk of reprisals, and would have a detrimental effect on a patient's mental state and create in them a feeling of distrust towards the health system.
- Disclosure of the information could reasonably be expected to prejudice the supply to LHD of confidential information that facilitates the LHD's functions.
- Disclosure of the information could reasonably be expected to prejudice the exercise of the LHD's functions (even if the information was not considered confidential).

Regarding the last two factors, the LHD submitted that:

- release of the footage would deter patients (and particularly patients with issues relating to mental health) from seeking treatment, and would inhibit their relationships with medical professionals; and
- in relation to SAR footage in particular, any disclosure of this footage could lead patients to refuse to be seen in these rooms due to confidentiality concerns, and this in turn would create a situation in which patients were seen in a less secure and safe environment.

The Tribunal considered each of the public interest considerations relied upon by the LHD, and the Tribunal's findings included the following:

- Release of the footage without pixelation would be in breach of privacy legislation (and health legislation in relation to Footage 1 which depicted a patient). However, if the face, head, neck, and any tattoos or other identifying marks of persons in the footage were pixelated, then the identity of those persons could not reasonably be ascertained, the footage would not be personal information or health information to which the relevant privacy and health records legislation applied.

- The evidence did not establish that there was risk of harm to hospital staff, security staff or patients if the footage were released in pixelated form (as described above).
- Footage 2 and 3, being recorded in public areas, did not record confidential information, nor did the events recorded by this footage form part of any patient's admission (such as to give it the quality of confidential information).
- Release of Footage 1 (in the SAR), even with the face, head and neck of all persons appearing in the footage pixelated, could reasonably be expected to have the effect of prejudicing the effective exercise of the LHD's functions. The Tribunal stated that:

  > A patient being interviewed by a doctor or other health professional within a SAR is entitled to expect that their interaction will remain confidential. In my view the public broadcast of any footage recorded in a SAR (or of events occurring in a SAR) will diminish patients' confidence in the confidentiality of their treatment and their interactions with health professionals. I consider this would be the case even if the footage is only broadcast with identifying features pixelated so that no identification of the patient is possible …
  >
  > [Such publication will] "create a risk that patients will be deterred from seeking medical treatment particularly where mental illness is a factor", and, perhaps more significantly, "undermine the use of SARs as safe spaces for the assessment of patients who present to emergency departments with potential mental health issues". If a doctor or other health professional cannot, with honesty, say to any patient in a SAR who might observe the CCTV camera, that the camera is there to ensure the safety of patients and others and that nothing recorded by the camera will be released publicly, that would have the potential to inhibit the efficacy of the provision of SARs and potentially discourage patients from attending a hospital.
- Disclosure of Footage 2 and 3, which records events occurring in public spaces, would not have the same effect as disclosure of Footage 1 (so as to diminish the likelihood that patients, including patients with mental health issues, would seek assistance at hospitals).

The Tribunal then balanced the public interest against disclosure as identified above, against the public interest in favour of disclosure. The Tribunal found that:

- There was an overriding public interest against disclosure of Footage 1 (which recorded an incident occurring in a SAR) even if the faces, heads and necks of the persons appearing in the footage were pixelated.
- The general public interest considerations against releasing Footage 2 and 3 without pixelation, arising from the disclosure of personal information and, potentially, health information, would outweigh the public interest considerations in favour of release of the footage. However, there were no general public interest considerations against release of Footage 2 and 3 with the face, head, neck and any tattoos or other distinguishing features of any persons appearing in the footage pixelated.

The Tribunal ordered that Seven Network be granted access to Footage 2 and 3 with pixelation as described above. The order was made on the basis that Seven Network would pay the costs of LHD retaining a third party to pixelate the footage.

Future Impact

This case demonstrates that pixelation could be used where video footage is requested under freedom of information legislation, but there are privacy, confidentiality, or public interest exemptions under the legislation that may apply to release of the footage in its raw form.

In this case, the Tribunal found that disclosure of the SAR footage (concerning events in a private patient area, rather than in public spaces) could reasonably be expected to have the effect of prejudicing the effective exercise of the LHD's functions, even where the footage was pixelated, as disclosure could discourage patients attending hospital. The Australian Capital Territory and South Australian legislation contain a similar exemption, which applies where disclosure would have a substantial adverse effect on the effective performance by an agency of its functions or operations.

In all jurisdictions, when dealing with requests for video footage, the other relevant exemptions are where the disclosure would disclose a person's personal information, or where the information was obtained in confidence and disclosure would be contrary to the public interest because it would impair supply of that information in future. In the

circumstances of this case, the Tribunal was not satisfied such exemptions applied where the footage could be pixelated, but these exemptions need to be considered on a case-by-case basis. Factors to consider may include whether the footage records a private or public location, and whether it records part of a patient's treatment or communications between patients and health professionals.

We note that freedom of information legislation in the Australian Capital Territory, the Northern Territory, Queensland, South Australia, Victoria, and Western Australia requires that, where practicable, access be granted to information with such deletions so as to make the information sought not exempt from disclosure.

There are no such express provisions under the GIPA Act in New South Wales or under freedom of information legislation in Tasmania, but provision of information with exempt material deleted is not precluded in these jurisdictions.

Organisations that are subject to freedom of information legislation will need to consider the practicality of pixelating or redacting footage to overcome any possible exemptions. In the Northern Territory, South Australia, Victoria and Western Australia, organisations may recover the costs of pixelating footage, but in the other jurisdictions the fees are limited to application fees and time-based processing fees only.

*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**.*

The Evolution of Telehealth in Australia, a Practical and Legal guide

Law Compliance has now produced the first in our White Paper series - Under the Microscope. The first issue focuses on Telehealth and m-health in Australia and is titled 'The evolution of Telehealth in Australia, a practical and legal guide'.

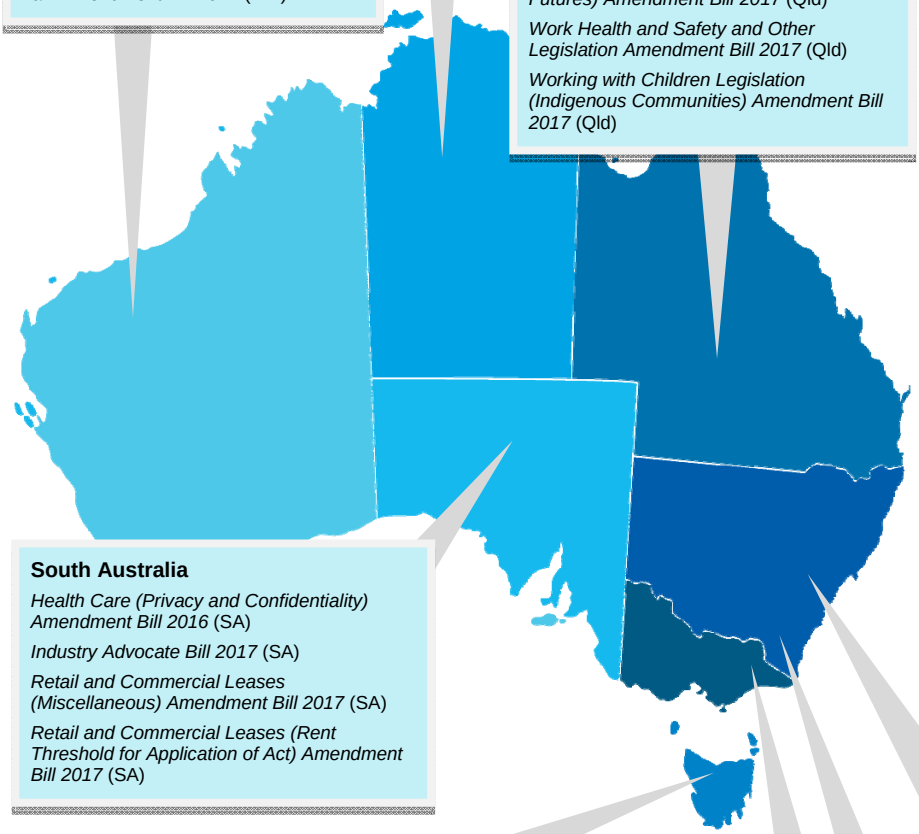
The Telehealth White Paper provides a snapshot of the existing spread of telehealth and m-health and associated technologies in Australia and explores the legal framework that applies to their use. The scope of the paper includes video consultation, mobile apps and devices, and wearable technology. The detailed legal obligations considered include privacy, standard of care, professional conduct, therapeutic goods and consumer protection.

The aim of the White Paper series is put a particular fast developing area of the law under the microscope.

If you are interested in obtaining a copy of the Telehealth White Paper, please contact ***Gwen Learey*** on (03) 98651323 *on **(03) 9865 1323** or **gwen.learey@healthlegal.com.au***.

LinkedIn® **Health Legal and Law Compliance are now on LinkedIn. Follow us for current news and updates.**

Some of the legislative changes being tracked



Northern Territory

Independent Commissioner Against Corruption Bill 2017 (NT)

Western Australia

Health Practitioner Regulation National Law Amendment Bill 2017 (WA)

Queensland

Child Protection Reform Amendment Bill 2017 (Qld)

Crime and Corruption and Other Legislation Amendment Bill 2017 (Qld)

Guardianship and Administration and Other Legislation Amendment Bill 2017 (Qld)

Hospital Foundations Bill 2017 (Qld)

Housing Legislation (Building Better Futures) Amendment Bill 2017 (Qld)

Work Health and Safety and Other Legislation Amendment Bill 2017 (Qld)

Working with Children Legislation (Indigenous Communities) Amendment Bill 2017 (Qld)

Commonwealth

Aged Care Amendment (Ratio of Skilled Staff to Care Recipients) Bill 2017 (Cth)

Australian Bill of Rights Bill 2017 (Cth)

Competition and Consumer Amendment (Competition Policy Review) Bill 2017 (Cth)

Competition and Consumer Amendment (Misuse of Market Power) Bill 2016 (Cth)

Corporations Amendment (Modernisation of Members Registration) Bill 2017 (Cth)

Fair Work Amendment (Corrupting Benefits) Bill 2017 (Cth)

Fair Work Amendment (Pay Protection) Bill 2017 (Cth)

Fair Work Amendment (Protecting Australian Workers) Bill 2016 (Cth)

Fair Work Amendment (Protecting Take Home Pay of All Workers) Bill 2017 (Cth)

Fair Work Amendment (Protecting Weekend Pay and Penalty Rates) Bill 2017 (Cth)

Fair Work Amendment (Recovering Unpaid Superannuation) Bill 2017 (Cth)

Fringe Benefits Tax Amendment (National Disability Insurance Scheme Funding) Bill 2017 (Cth)

Higher Education Support Legislation Amendment (A More Sustainable, Responsive and Transparent Higher Education System) Bill 2017 (Cth)

Imported Food Control Amendment Bill 2017 (Cth)

Industrial Chemicals Bill 2017 (Cth)

Industrial Chemicals (Consequential Amendments and Transitional Provisions) Bill 2017 (Cth)

Industrial Chemicals (Notification and Assessment) Amendment Bill 2017 (Cth)

National Disability Insurance Scheme Amendment (Quality and Safeguards Commission and Other Measures) Bill 2017 (Cth)

Privacy Amendment (Re-identification Offence) Bill 2016 (Cth)

Treasury Laws Amendment (Improving Accountability and Member Outcomes in Superannuation Measures No. 2) Bill 2017 (Cth)

South Australia

Health Care (Privacy and Confidentiality) Amendment Bill 2016 (SA)

Industry Advocate Bill 2017 (SA)

Retail and Commercial Leases (Miscellaneous) Amendment Bill 2017 (SA)

Retail and Commercial Leases (Rent Threshold for Application of Act) Amendment Bill 2017 (SA)

New South Wales

Children and Young Persons (Care and Protection) Amendment (Auditing of Out-of-Home Care Providers) Bill 2017 (NSW)

Human Tissue Amendment (Trafficking in Human Organs) Bill 2016 (NSW)

Summary Offences Amendment (Safe Access to Reproductive Health Clinics) Bill 2017 (NSW)

Voluntary Assisted Dying Bill 2017 (NSW)

Tasmania

Care and Consent to Medical Treatment Bill 2016 (Tas)

Expungement of Historical Offences Bill 2017 (Tas)

Voluntary Assisted Dying Bill 2016 (Tas)

Victoria

Disability Amendment Bill 2017 (Vic)

Drugs, Poisons and Controlled Substances Amendment (Real-time Prescription Monitoring) Bill 2017 (Vic)

Health Legislation Amendment (Quality and Safety) Bill 2017 (Vic)

Long Service Leave Bill 2017 (Vic)

Residential Tenancies Amendment (Long-term Tenancy Agreements) Bill 2017 (Vic)

Voluntary Assisted Dying Bill 2017 (Vic)

Australian Capital Territory

Justice and Community Safety Legislation Amendment Act 2017 No. 5 (ACT)

Workplace Privacy Amendment Act 2016 No. 22 (ACT)

If you would like details of these new Bills please contact ***Teresa Racovalis*** *on* ***(03) 9865 1337*** *or* ***teresa.racovalis@lawcompliance.com.au****.*

Staff News

Naj Uyanik joined Health Legal at the end of June 2017 as a Junior Administrative Assistant. Naj provides administrative support to both the Health Legal and Law Compliance solicitors and has already proved to be an invaluable member of the team.

Fiachra Twomey joined Health Legal's growing compliance team in August 2017. Fiachra has recently graduated from La Trobe University and will complete his Practical Legal Training while working at Health Legal. As part of Health Legal's compliance team, Fiachra reviews and updates the legislative compliance products produced by the firm.

Welcome Naj and Fiachra!

Useful information links

At Health Legal we regularly access a broad range of information to ensure we keep up to date on what is happening in our areas of interest, both here in Australia and overseas.

In each publication we will share some of our regularly accessed sources of information, which we believe our clients will find useful. The links we would like to share this time are:

- **http://foicommissioner.vic.gov.au/**
  is now the home page of the Office of the Victorian Information Commissioner.
- **https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/**
  provides information on the notifiable data breach scheme to come into effect in February 2018.
- **https://www2.health.vic.gov.au/about/publications/policiesandguidelines/simplifying-medical-treatment-decision-making-and-advance-care-planning-position-paper**
  useful background information to the *Medical Treatment Planning and Decisions Act 2016 (Vic)* to come into effect in March 2018.
- **http://www.ibac.vic.gov.au/reporting-corruption/notifications/information-for-principal-officers**
  provides information for Victorian principal officers regarding mandatory notification of corrupt conduct.
- **https://www.nhmrc.gov.au/health-topics/genetics-genomics-and-human-health/genetics-and-genomics-resources-clinicians-and-rese**
  provides comprehensive information for health professionals on genetics and genomics.
- **https://www.fairwork.gov.au/**
  includes best practice guides and a variety of resources for employers to assist in compliance with the FWA.
- **http://www.alrc.gov.au/**
  provides an interesting update on the elder abuse inquiry among other matters under consideration.

Compliance Subscribers

Our compliance team are in the midst of obtaining feedback from all legislative compliance subscribers and are gathering expressions of interest in attending a workshop/forum on the products and services currently offered. We will be conducting one for users of our Word based product and others specifically for those who access our content via RiskMan or Advent Manager. If you are interested in attending any of the forums (likely to be a half day), please contact ***Jeremy Smith*** at ***jeremy.smith@healthlegal.com.au***.

Contact us

For further information please contact:

Natalie Franks
Legal Counsel
Direct: 03 9865 1324
Email: natalie.franks@healthlegal.com.au

Claudia Hirst
Legal Counsel
Direct: 03 9865 1340
Email: claudia.hirst@healthlegal.com.au

Alon Januszewicz
Associate Legal Counsel
Direct: 03 9865 1312
Email: alon.januszewicz@healthlegal.com.au

Sarah Caraher
Senior Associate
Direct: 03 9865 1334
Email: sarah.caraher@healthlegal.com.au

Teresa Racovalis
Chief Operations Officer (Compliance)
Direct: 03 9865 1337
Email: teresa.racovalis@lawcompliance.com.au

Astrid Keir-Stanley
Compliance Associate
Direct: 03 9865 1329
Email: astrid.keir-stanley@lawcompliance.com.au

Giovanni Marino
Senior Solicitor
Direct: 03 9865 1339
Email: giovanni.marino@healthlegal.com.au

Anne Howard
Solicitor
Direct: 03 9865 1311
Email: anne.howard@healthlegal.com.au

Ksandra Maruna
Compliance Solicitor
Direct: 03 9865 1320
Email: ksandra.maruna@lawcompliance.com.au

Chris Chosich
Solicitor
Direct: 03 9865 1343
Email: chris.chosich@healthlegal.com.au

Jeremy Smith
Compliance Solicitor
Direct: 03 9865 1342
Email: jeremy.smith@healthlegal.com.au

Fiachra Twomey
Law Clerk
Direct: 03 9865 1343
Email: fiachra.twomey@healthlegal.com.au