First, do no harm: Privacy in healthcare delivery

Privacy Commissioner, John Edwards' speech

to Waitemata DHB

20 July 2015

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about" – Hippocrates.

This promise embodied by the Hippocratic Oath is as important today as it has ever been. Patients expect that their precious personal information will be treated with total respect, and I would be very surprised if doctors expected any less.

That's because health information is highly sensitive and confidential personal information and the protecting it against disclosure is an inevitable part of the delivery of health and social services.

Hippocrates and his ilk knew this and we know this today, nearly two and a half thousand years later.

But here's the difficulty. Hippocrates never had a risk manager, or auditor, or funder or professional association. He was never a member of a PHO, or child protection team. He didn't have coroners, politicians or officials blaming him for terrible outcomes "because he didn't share information".

Of similar venerability, if slightly less certain provenance is the injunction "First do no harm". I've always admired its deceptive simplicity. It is deceptive because it can be read as a call to inaction, "don't take the risk?" But what if the inaction causes the harm? What kind of harm are we to avoid? Should we do no harm because of a legal risk, such as breaching the Privacy Act when the benefits of taking action far outweigh the legal consequences of making the wrong call?

The words "do no harm" resonate with me because they form a key part of the Privacy Act. While everyone in New Zealand – including medical practitioners – are obligated by law to follow the rules in the Act, liability can only be established when there has been a clear "interference with privacy." An interference with privacy usually has two main components.

First, one of the 12 privacy rules has to have been broken.

Second, an individual has to have experienced harm as a result of that rule being broken. Harm is not restricted to physical or financial harm. Harm can be an adverse effect on rights, privileges or obligations. It can be significant humiliation or loss of dignity. It can be significant injury to feelings.

There are two notable exceptions: rules 6 and 7. These rules relate to an agency's obligation to provide individuals with information held about them when asked, and correct any incorrect information held about individuals.

In circumstances where agencies fail to follow rules 6 and 7, the individual does not need to demonstrate harm – the breach alone is enough to create an interference with privacy.

With this in mind, I want to explore the different forms of harm that can be caused through privacy breaches, give some guidance to help avoid those situations in your day-to-day work, and speak about ongoing developments in this area.

Patient notes and handover

I remember speaking to a group of nurses in the early days of the Privacy Act. This was when patient notes were kept on a clipboard at the end of the bed. Anyone walking by could have a look, regardless of whether they needed the information or not.

One of the nurses asked me whether this setup constituted an interference with privacy. Lacking an immediate answer, I put it back to them, and asked the crowd to pipe up with what information they would rather not see disclosed; in other words, information that would cause harm if someone else knew it.

“My age!” was the first response, with murmurs of agreement. Then someone else said “I don’t care if people know my age . . . but I don’t want them knowing my weight!”

Then it felt like the whole room started chipping in, all with different bits of information on their charts that they would rather be kept private.

This neatly illustrated how subjective privacy can be. Any information leaking without consent is a potential source of harm – regardless of how banal or irrelevant the information appears.

Practically speaking, it means patient notes should be protected, but not necessarily under lock and key. Information like this is a balancing act between giving medical practitioners the ability to access the data they need, when they need it and protecting patient privacy from passers-by.

Taking information offsite

A privacy breach doesn’t have to be deliberate to become an interference with privacy by causing harm.

Late last year, one of my senior investigating officers came to me with a file she’d been working on.

What had happened was that a health worker out on her rounds had her car broken into. Her notebook was in the car. In the notebook were details of some 90 clients she had seen in recent years.

Her employer, a DHB, did the right thing, and got in touch with all the clients, to let them know what had happened. Some of them were accepting of the error, some were a bit upset, but the one who complained to us was devastated by the breach.

It had been some years since this one client had seen the health worker and she could not understand why she would still be carrying around her extremely sensitive personal information, which revealed details of mental ill health following the birth of a child.

Often, if a third party like a thief intervenes maliciously to release personal information, it would not be fair to hold the agency responsible.

But in this case, we had to consider whether the agency had taken reasonable steps to ensure the information was protected from loss.

Health Information Rule 5 of the Health Information Privacy Code says an agency that holds medical information shall ensure that the information is protected by such security safeguards, as it is reasonable in the circumstances to take, against loss or disclosure.

While we acknowledged that there would be cases where it was necessary to take patient information 'offsite' when treating patients in the community, we were not satisfied it was reasonable to expose this type of historic information by taking it out of the DHB.

It's worth mentioning that the DHB had very clear processes around patient files, which were not allowed off the premises. However, the same safeguards were not applied to the notebooks that healthcare workers used, which copied a substantial amount of sensitive information from those files. When the notebook went missing, a patient was harmed.

In an effort to resolve the complaint, I met with with the chief executive of the DHB. We had a very productive conversation and were able to agree to terms on which the complaint would be settled without referral to the Director of Human Rights Proceedings.

In this conversation, I learned that the DHB's biggest concern was the perception that we were requiring a significant change of professional practice - namely that we were saying patient information should never be taken offsite.

A "ban" on taking information offsite would have had significant, potentially harmful implications on the ability for the DHB to function given the shift in clinical service delivery to community care.

The reality is that privacy should *follow* practice, rather than dictating it. The Privacy Act should be integrated into the way you do your job rather than stop you from doing your job.

With this in mind, we undertook to provide some guidance to help health workers and others who are increasingly mobile reduce the risks of interfering with privacy:

- if possible, transport patient notes or information in a secure container and remain in touch with them without ever leaving them in open view or on a seat
- only take the notes you need for your task
- if it's a rainy or windy day, secure the notes in a bag, so they don't blow away or get wet
- the same goes with securing BYO devices; and
- don't take notes out for an extended period, when you don't need them.

It concluded that, just as you don't leave your valuables, such as your wallet, in your car, treat patient notes and information the same way.

We're still working through our guidance for these scenarios, so get in touch if you want to weigh in. We're seeking consultation from all the DHBs.

Hammond v NZCU Baywide

The lost notebook case was ultimately settled. However, another case that went to the Human Rights Tribunal is a useful example of how our society is placing an increasingly higher value on privacy and the harm a breach can cause.

A few years ago, a woman shared a photo with a limited number of friends on Facebook. The photo featured a cake with written obscenities referring to NZCU Baywide, her employer at the time.

The photo was obtained by NZCU Baywide managers and disclosed widely, in what was described by the Tribunal as a "sustained campaign by the company to inflict as much harm and humiliation as possible by ensuring Ms Hammond could not be employed in the Hawkes Bay area" and to get her dismissed by her subsequent employer.

The Tribunal said it had established that loss, detriment, damage or injury, as set out in section 66 of the Privacy Act, had occurred to Ms Hammond. It was also satisfied that there had been significant humiliation, loss of dignity and injury to her feelings. It awarded her a record $168,000 judgement -- $98,000 of which was due to the emotional harm NZCU Baywide caused by breaching Ms Hammond's privacy.

So there's certainly a lot to lose by getting it wrong. Not only are they out nearly 170 thousand dollars, the judgement and a news story about the case are on the first page of Google's results for the company's name. That reputational damage is going to linger, and probably cost them a lot more than $170k.

Here's what's really interesting about the whole debacle: The HRT only found that NZCU had interfered with Ms Hammonds privacy distributing the screenshot. Downloading the screenshot wasn't an interference. Neither was discussing the screenshot internally. Neither of these actions harmed Ms Hammond. Distributing the screenshot to recruiters and others did harm Ms Hammond.

You can use this case as a rule of the thumb. When you share information about a patient, are you "doing no harm" ? If you take a picture of a patient's injury on your phone to get feedback from a colleague, could that harm the patient?

Probably not – but if you shared it on social media, you could absolutely cause harm. And like I discussed before, an interference with privacy doesn't have to be deliberate. When you plug your phone into your laptop, does it automatically sync? Do you upload your photos to a cloud storage service? If so, what are the privacy settings?

These are the kinds of questions you need to ask yourself. Good intentions are not enough. You need to make sure you've taken the necessary steps to give privacy the same treatment that underpins your medical training: "first do no harm."

Petition and the rights of minors

Those examples cover the enforcement side of my office's responsibilities, but we also devote substantial resource to looking forward. The two main ways we do so are:

1) providing educational resources and guidance
2) advising on the privacy implications of new laws and policies

I want to speak for a moment on this second point.

Right now, there is a petition in front of Select Committee asking Parliament to pass legislation compelling medical practitioners to seek parental consent for any procedure they advise for pregnant patients under the age of 16.

Let's be clear: they're talking about terminations.

The petitioners argue that anyone under the age of 16 is a child, and therefore their parents have a right to their medical history.

They are partly right. The Health Information Privacy Code gives parents the presumptive right to medical information about children under the age of 16.

In practice, things are not so cut and dried. There's no switch that flicks on someone's 16th birthday that grants them competency and understanding that they didn't have the day before.

This is why there are exceptions to that presumption. When a child asks for confidentiality, the medical practitioner makes the judgement as to whether a patient can consent to a procedure on her own, or whether her parents need to be involved in the decision.

Taking this discretion away from medical practitioners has the potential for unintended consequences.

Could it encourage young women to lie about their age and compromise their care?

Could it encourage unsafe alternatives?

What issues could arise from a situation where a medical practitioner's legal obligations to the state are pitted against his or her ethical obligations to the patient?

Would it strengthen, or impede, the medical practitioner's obligation to "do no harm"?

Making privacy easy

On the compliance and education side of things, I want to 'make privacy easy'. This is my vision as Privacy Commissioner.

I want to find out the significant issues in your sector and give you the tools you need to comply with the law. Whether it is checklists, consumer friendly privacy policies or guidance notes, I want to do it once so you and your colleagues can use it many times.

We already have a significant investment in making privacy easy for you, including an 0800 number with enquiries staff fielding around 9000 calls per year offering immediate practical assistance.

These are some of our particularly relevant initiatives in this space:

A Health 101 module in our online training, which was developed by educators and privacy specialists. It gives a clear understanding of the rights and obligations as a healthcare professional under the Privacy Act.

The online training is free and you can do it from anywhere, at your own pace. You should do it – and encourage others to do it as well. I expect to see it in induction material and in ongoing professional development. The time spent is absolutely worth it in relation to the potential costs that can stem from interfering with someone's privacy.

A toolkit for Privacy Impact Assessments. This is a framework that helps you find the potential privacy issues when you're changing systems, processes or policy. If you haven't done one before, it's worth doing one now anyway – you'll unearth any potential privacy problems in your current processes so you can fix them before you find yourself in breach for harming someone.

Our *Sharing Personal Information of Families and Vulnerable Children* guidance and its accompanying interactive information sharing Escalation Ladder tool – for people and agencies who work with vulnerable children.

Approved Information Sharing Agreement (or AISA) guidance to assist government agencies that want clear and precise guidelines around what information can be shared and with whom.

We've also created an online privacy statement generator that helps you generate your own privacy statement in 5 minutes. The organisations you work for probably already have privacy statements, but I encourage you to try it anyway – it's a really good way to get a broad-brush view of what you need to think about when it comes to privacy.

All these resources are available on our website.

This brings me to the furthest look forward – the coming law change to the Privacy Act.

Law reform

The draft legislation is based on a five year long review carried out by the Law Commission on the privacy laws. It is likely to go before Parliament later this year.

The Law Commission made about 140 recommendations and the Government has accepted the majority of those recommendations. The intention is to modernise our 21 year old privacy laws to make them more future-facing.

Mandatory breach notification

Many agencies do currently alert us to data breaches but that requirement is voluntary under the current law. In the case of the data breach I discussed earlier (with the stolen notebook), the DHB was not the party that alerted us it, it was the complainant.

One significant aspect of the forthcoming law change will be the introduction of mandatory breach notification. Agencies will have to notify us if they experience a serious data breach.

New Zealand is unusual internationally by having a voluntary system. We currently receive numerous (and growing) voluntary breach notifications. These depend upon the willingness of agencies to alert us if there's been a data breach.

We have started to track breach notifications more formally and report on them. This information can be found in our annual report.

Under the proposed reforms to the Privacy Act, actions such as failing to notify me of a privacy breach, or impersonating someone to obtain their personal information will be illegal and carry a fine of up to $10,000.

Existing maximum fines - for example, for obstructing my office - will increase from $2,000 to $10,000.

Other enforcement powers that my office will get in a new Privacy Act include:

Access determinations

I will have the power to order that information be given to people through access determinations. This is a very significant change because over 60 percent of the complaints that my office receives concern requests for access.

I can't stress this enough - providing access is a key part of any business, a key part of the relationship between an agency and its clients. It is not some legal compliance exercise.

Enforcement notices

Another major tool that my office will get is the power to issue enforcement notices to non-compliant agencies.

I'd expect this to be a tool that will be rarely used, and probably as a last resort, but it is notably lacking from the current range of enforcement options.

Conclusion

A common theme we see in the media is an idea of "safety vs privacy." It's a helpful dichotomy, but it's overly simplistic. The reality is that you can have it both ways.

As healthcare workers, you don't need to compromise privacy to create safety through better health outcomes, and privacy doesn't need to impinge on your ability to deliver the best possible outcomes. Rather, the two concepts work together to accomplish the same goal: to first, do no harm.