The temptation of inappropriate employee browsing

CCDHB Grand Round

John Edwards, Privacy Commissioner

University of Otago, Wellington

Introduction:

"Make a habit of two things - to help, or at least to do no harm."

That statement is attributed to Hippocrates, the forefather of modern medicine.

The words "do no harm" resonate with me because they form a key part of the Privacy Act.

Hippocrates also reportedly said "physicians are many in title but very few in reality".

This is perhaps a reference to the number of charlatans in classical Greek society who purported to be doctors.

If these charlatan practitioners were more common than doctors, it is likely that there was a great deal of harm caused in the name of medicine in those days.

But the harm I want to talk about today is harm as a function of an interference with privacy – particularly inappropriately accessing patient records. This is more commonly known as employee browsing.

Harm is not restricted to physical, emotional or financial harm.

Harm can also 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.

I want to talk about what employee browsing is, talk about some cases to show how harmful it can be, then give some advice to prevent employee browsing.

Defining employee browsing

I want to start by establishing what we're talking about when we talk about employee browsing.

Let's say you're searching for a patient with a common last name. Call him Mr. Jones.

You type in his last name, and, predictably, uncover a lot of Messrs. Jones.

You click through a few of them until you find the right Mr Jones.

Don't panic: I'm not going to tell you that you can't do this. This is not inappropriate access. This is just doing your job.

Here's another example. Say there's someone famous in the hospital. An All Black, for example.

He’s not your patient, but you’re a keen rugby fan. So you look him up to see the extent of his injuries.

This is not appropriate. This is the kind of employee browsing I want to talk about.

We all remember the case of the former Black Caps cricketer, Jesse Ryder, in 2013.

Four clinicians were disciplined by the Canterbury DHB for breaching patient confidentiality.

The CDHB investigation found there had been a total of seven breaches to Ryder's X-ray records by staff not involved in his case.

As health professionals, this is the kind of browsing that serves no purpose towards the duty of care you have towards your patients and can cause significant harm to that patient.

Dignity

A breach of trust of this nature relates closely to the concept of human dignity.

Patients that trust their medical providers are more willing to engage with them.

They’re quicker to make appointments, and they’re more candid when they know that their problems will be treated with discretion and dignity.

When you respect your patients’ personal information, you help them to trust you.

A breach of this trust is an affront to their dignity and risks the confidentiality that is one of the foundations of your duty of care towards your patients.

Run-of-the-mill information

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 volunteer 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.

That’s because regardless of how banal or irrelevant the information might appear to one person, it might be highly sensitive to another.

What if they never found out?

But how can people be harmed by employee browsing if they never find out?

There are a few reasons why this argument doesn't stack up.

Let's pretend I've sent a colleague to your house.

He or she will look around, make some notes, take some pictures. They'll wipe their feet when they enter and put everything back as they found it. You'll never know they were there.

Is this acceptable?

What if my colleague was occasionally caught? Would you assume it was an isolated circumstance?

Or would you be concerned about the possibility that this had happened before?

The effect of employee browsing is a kind of death to trust by a thousand cuts – where patient trust is eroded a little bit more each time it is revealed that someone in the system has been accesses records they shouldn't be accessing.

Even if the individual patient never finds out, the fact that it's happening has the impact of reducing the overall reservoir of patient trust.

Eel case

And when patients do find out that it happened to them, the effect can be traumatic.

You may recall a few years ago, when an Auckland man came to the ED with an eel in his bowel. I won't get into the details of how it got there.

The man's X-ray was emailed to a significant number of people, and word of his predicament quickly got out to the public and the media.

49 employees were investigated and 33 were disciplined. Some lost their jobs.

This is not what the patient came to the hospital for. He came to be treated for a condition – just like every patient.

He did not come to the hospital to be gossiped about and embarrassed.

The staff who accessed and distributed his information probably assumed he would never find out. But he did, and harm was done.

CCDHB case

Another example concerns an employee who used to work at this hospital in an administrative role.

She had naturally been a patient of the CCDHB at different points in her life.

After she finished working here, she was notified by the DHB that one of her ex-colleagues had been browsing her records.

This had happened on numerous occasions in 2012 and 2013.

The knowledge that her records had been browsed gave additional context to comments that colleagues had made when she worked here.

She asked for an audit of her records to see how far the browsing went, and found that *another* former colleague had also browsed her records.

This was compounded by the fact that the information in question was extremely sensitive emergency department and mental health information.

As a result, she suffered high levels of anxiety, nightmares and a complete erosion of her trust in this DHB.

Browsing someone's records inappropriately can be a ticking time bomb. There may be no harm today, tomorrow or this year, but it can emerge years later.

When the patient does find out, it can change their perception of events; it can make them re-examine conversations and interactions with colleagues with a critical eye, turning old memories into negative memories.

When a patient no longer trusts a hospital, that patient is less likely to seek out medical services from the hospital in the future.

They may even lose trust in health and social services in general, and be less willing to engage with a number of different organisations.

The trauma of employee browsing also impacts further than the individual.

Even if the direct victim is able to trust the hospital again, that may not be the case for those who hear or read about employee browsing incidents.

How long will a sick person wait before seeing a medical professional if they don't trust professionals with their information?

How much more advanced will their condition become as they weigh up the potential emotional trauma against their physical, growing pain?

These are the potential consequences of inappropriately accessing records.

Non-digital cases

Most of the conversations around inappropriately accessing patient records tend to focus on digital scenarios. Emails sent around, databases accessed and so on.

But patient records aren't limited to digital record-keeping systems.

One case my office dealt with a few years ago involved an administrative staff member who was typing dictated notes from a surgeon.

The notes turned out to be about a friend of hers, who was very sick.

She passed on her condolences to the friend, who complained to us. The hospital ended up paying a settlement.

This case shows a couple things.

One is that patient information is not limited to computers. It can make its way through every communications channel there is.

The next lesson here is that inappropriately using or seeing patient information can come from the best of intentions.

It's not always a callous or malicious act, but the harm can be significant either way.

The cost of getting it wrong

Infringing on someone's privacy can also have direct economic costs.

This case isn't in a healthcare context, but it shows how expensive and time-consuming a breach can be.

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, a Hawkes Bay credit union and her employer at the time.

The photo was obtained by NZCU Baywide managers and disclosed widely.

The woman made a complaint to our office which made its way to the Human Rights Review Tribunal.

The Tribunal awarded her a record 168 thousand dollars – of which nearly 100 thousand was for the emotional harm that NZCU Baywide caused the woman by breaching her privacy.

There was also substantial reputational damage to the company caused by the media coverage the case received.

Rule of thumb

You can use this case as a rule of the thumb. When you browse patient data, are you doing so to do your job? Or are you browsing for another reason?

If you looked up a past case to help diagnose the patient in front of you, or looked at patient information as part of your ongoing training, would that be a problem?

Probably not - but if you looked up a case that someone forwarded to you out of pure interest, that may be over the line.

Think it over carefully before you look up, copy or share patient information.

I cannot imagine the finance team would be thrilled if you broke the HRRT's new $168,000 benchmark for Privacy Act damages.

What do we do about it?

The situations I gave seem clear-cut in retrospect, but the day-to-day of delivering healthcare is much more nuanced.

IT systems with sufficient audit and oversight mechanisms are a start.

They can find the most obvious and egregious examples, such as a patient file being accessed dozens of times.

A number of DHB's have what I call an "A list" and a "B list" of patients.

The "A" list is celebrities, politicians, business leaders and other people of prominence.

The system flags whenever these patients' records are accessed.

I don't like this approach, because it creates a situation where prominent peoples' privacy is given greater care and protection than everyone else's privacy.

Privacy is for everyone, not just those with recognisable names.

But IT systems won't help you when an employee is looking up their daughter's boyfriend or their neighbour.

IT systems are only as effective as the parameters that are set for them by the IT department and the system administrators and these parameters in the majority of cases cannot detect most cases of employee browsing.

This is not to discount IT systems altogether. While their ability to detect inappropriate access ahead of time is limited, they do give the ability to audit access in retrospect.

This is a major improvement from the days of paper-based records, when it was quite possible to look at a file without leaving any trace of your presence.

As I mentioned in the case about the CCDHB administrative employee, digital footprints or trails can be valuable in the event of an incident, to find out how far the inappropriate access went.

DHB's can also use these tools as part of their audit processes to detect inappropriate access.

But they work retrospectively, not preventatively, and it's important to bear that in mind.

Building a culture of privacy awareness

Day-to-day behaviour within an organisation needs to be influenced by the organisation's overall culture around personal information.

A culture of privacy awareness is the best way to prevent employee browsing and other privacy breaches, as well as manage breaches if they do happen.

It needs to be deeply embedded at every level of your organisation.

Grow a culture of awareness

As a privacy regulator, here's a checklist of some of the sorts of things that I will be looking for in the event that things go wrong:

- Organisational culture and awareness of good privacy practice
- Levels of training for staff
- Sensible, clear policies and privacy statements
- Awareness of data breach notification and mitigation

If we are investigating a complaint against your organisation, these elements will become relevant and if your organisation has got its privacy mix right, it will reflect well on your organisation.

E-learning

Privacy education is a key foundation for privacy awareness. To help with this, we've developed online training modules.

In the past, we used to deliver in-person privacy training to small groups..

But you can only fit so many people into a room, and people are busy: a half day or more can be hard to find in the schedule.

In order to give more people access to this training, we worked with a group of professional educators called LearningWorks to apply our in-person content to an online context. This time last year, we launched online training modules, which we've dubbed e-learning.

The training is available on our website for free. Rather than find hours in your schedule and travel to an office, you can pick up and put down the training when it suits you. You can do 10 minutes here, half an hour there.

It's also worth professional development hours for some clinical staff and lawyers.

There's a module – called Health 101 – devoted to the Health Information Privacy Code. I encourage everyone in this room to take the time to undertake this training.

When my office receives privacy complaints, we often look into whether the agency in question had taken reasonable steps to avoid the privacy breach in question.

We tend to look much more favourably on those who have taken the time to educate their staff than those who have not. And at the same time, agencies with educated staff tend to have fewer privacy issues in the first place.

Engage with us online

Over the past couple years, we've changed the way our office works by engaging and interacting with more people online.

There are a wide variety of resources on our website, such as guidance documents, case notes and blog posts.

We use our blog, Twitter, Linked In, YouTube and Facebook channels. We update these channels all the time – the blog a few times a week, Twitter several times a day.

I encourage you to follow these channels and stay up to date with what's happening in the privacy world.

By regularly checking in, you start to develop more privacy awareness, which will help you make the right decisions in practice..

Privacy Week

Our annual Privacy Week is next month. This is a week with a variety of different activities, both from us and other agencies.

For example:

- We will be curating an online exhibition of privacy-themed art by artists from five community art workshops. This is a continuation of a project we did during Privacy Week last year. I encourage you to take a look at what they come up with.
- We'll be publishing the results of our latest UMR survey on public attitudes towards privacy and data protection. We expect that public awareness of privacy will be high, as it has been rising for the past few years.
- A number of new privacy resources and publications.
- A visit from UN Special Rapporteur for the Right to Privacy, Joe Cannataci.

Keep an eye on our website and follow us on social media to stay up-to-date.

Looking forward – law reform and naming policy

On the horizon, there is also upcoming law reform to the Privacy Act. There is one particular component you should be aware of.

One of the expected changes to the Act includes mandatory breach notification.

This means that organisations – including this one – will be required to tell my office when they find a privacy breach, such as employee browsing.

A law change in the area of breach notification would be a significant game changer.

Why? Because it shifts business expectations and creates a level playing field for all across the public and private sector.

It also gives a better macro view of privacy breaches.

Breach notification is currently voluntary. We received 121 in the last financial year, and 116 in the year before that. The problem is, we don't know what proportion of total breaches that represents.

Is it 121 out of 125? Is it 121 out of a thousand?

The answer is probably somewhere in between, but without mandatory notification we don't have the ability to do much more than make educated guesses.

The time frames for legislative change are uncertain. So, in the meantime, we are making robust use of the enforcement tools we currently have as a regulator.

For instance, we have introduced a policy on naming agencies that in our view deliberately, systematically or consistently flout the law.

But as I've mentioned, if investigating any complaint, and I find that you have a good organisational culture, an awareness of good privacy practice, staff who have received some privacy training, and clear and sensible privacy statements, then I'd be more inclined to find in your favour.

It's also in the interests of your patients and the wider community.

A culture of privacy awareness reduces inappropriate employee browsing.

A DHB with less employee browsing is more trustworthy.

And a trustworthy DHB is one that people are more willing to engage with – early, often and with full disclosure.