PO Box 745 Indooroopilly QLD 4068 AUSTRALIA
**Ph 1300 662 173 or +61 7 3378 2668**
Email stenography@pacifictranscription.com.au
Web www.pacifictranscription.com.au

# MEDICO-LEGAL SOCIETY OF NSW INC.

## SCIENTIFIC MEETING

## WEDNESDAY, 20 SEPTEMBER 2017

## AT 6.15 P.M.

## THE TOPIC:

## ONCE MORE UNTO THE BREACH

## PRIVACY UPDATE:
## MANDATORY DATA BREACH NOTIFICATION
## AND THE HEALTH PROFESSIONALS

## QUESTION AND ANSWER PANEL DISCUSSION

**PANELISTS:** MR ANNAN BOAG
MS ALISON CHOY FLANNIGAN
DR WALID JAMMAL

**FACILITATOR:** DR JULIAN WALTER

**DR JULIAN WALTER:** There is quite a lot to cover this evening and I'd like to use the time as best we can. By way of introduction, I'm Julian Walter, I am going to convene this session. I'm a medico-legal advisor from MDA National, so both solicitor and doctor and have a bit of an interest in the topic. We've had a few discussions about this over time and it's great to have the opportunity to actually run some of these scenarios past our panel.

Beside me we have a bit of a 'Dream Team' in terms of privacy issues. I won't read through these bios but we have Annan from the Office of the Australian Information Commissioner. It's very good of him to come along. He replaces Paula, who is in the program, her expertise was more in My Health and this discussion is going to be a bit more about data breaches and privacy, and that is an area that Annan works in.

His area of expertise, he's dealt with some fairly large-scale privacy breach investigations, the Red Cross breach and also the dating website, Ashley Madison, which if you can't remember, was in 2015 where some 37 million subscribers to that dating site's details were hacked and released - we think we have problems in health.

He can probably give us some insights into the way such large breaches are managed. He is also currently implementing Australia's notifiable data breach scheme, which is what we're going to be talking about.

Next is Alison. Alison is a partner with Holman Webb. She has 20 years' experience in the health law area and she is my go-to person in terms of privacy issues, whenever we have them, so it's fantastic to see her here.

She too has been involved in all sorts of privacy related problems, including advising what was NEHTA and is now the Australian Digital Health Agency, who are setting up the My Health Record and the trial sites.

Then Walid, I've known Walid since 1994 when he was my registrar in intensive care. Walid is a general practitioner. He owns a practice, which I think he's owned since 2001 and has also just recently been awarded the NSW ACT RACGP GP of the Year.

Walid also works at Avant as an advisor in their advocacy section and lectures in medico-legal issues.

It was over a year ago when we started looking at topics for this year and privacy came up as a possible topic. At that

time, the data breach legislation hadn't passed and when we started thinking about what we might talk about, it wasn't necessarily clear what we would fill the night with.

In the meantime, the data breach legislation has passed and we put questions out to the membership to find out what they wanted to know about privacy and also some of our colleagues in the office. It became apparent that the forthcoming data breach notification requirements starting next year was an issue of interest to a lot of people.

We thought rather than presenting just what the legislation is, which is not that interesting to just to read through slabs of legislation, we thought we would start with some scenarios and work out whether we might be notifying this to the Australian Information Commissioner or not.

It's actually been very educational to me. When I started this, I thought I would be making a lot more notifications or helping doctors make notifications next year than probably is the case; so, it's been very beneficial to me working through these issues.

Where are we now? There is absolutely no doubt that there is a huge expectation by the community, the regulators, the media, the profession, that the information with which we deal, so- our patients' health information, is kept private and confidential.

I'm not so sure we do it that well and a brief look of the news media reveals an enormous number of breaches. Most of these articles up here come from this year. Thankfully, most of them are hospitals rather than private practices which is perhaps where the legislation is going to apply more relevantly, but there are plenty of examples where patients' records have been left out on the street or sent places where they shouldn't and incredibly sensitive information has been released.

It's not just hospitals. You can also find plenty of examples of information from general practitioners, perhaps less so than hospitals.

That brings us to our first scenario tonight where a breach prompted the Office of the Australian Information Commissioner to comment. This is from Timothy Pilgrim. I don't know if you remember, this was the Pound Road Medical Centre breach, where a doctor left their records stored in a garden shed which was broken into and the records became available. The comment was made there, "I can't think of

any circumstances in which it would be reasonable to store health records, or any sensitive information, in an insecure, temporary structure such as a garden shed."

We are going to presume in our scenario that we've moved on a bit from the garden shed. We're going to talk about Walid's theoretical practice where it's a very technical practice, he has passwords on all of his software, everything is encrypted, he looks after his practice well.

We're going to use Alison as our legal advisor if he has problems and Annan's going to stay in his role as the worker in the OAIC who's potentially going to advise us about what to do in some of these scenarios.

I thought I would get a bit of an idea, probably Annan you can help me here, as currently the legislation hasn't come into force. What happens if I have a data breach currently, do I need to tell you?

**MR ANNAN BOAG:** You're right, there is no requirement at the moment to notify people who are affected by a data breach or the Australian Information Commission if one has occurred. That is not to say you shouldn't and that a lot of people don't at the moment.

We generally recommend that if it's a serious data breach, particularly if there is a risk of serious harm to the people who are involved, you should think seriously about letting them know. It is increasingly a community expectation. OAIC's Community Attitudes to Privacy Survey 2017 found that something like 95 per cent of the Australian community thinks that they should be notified if their personal information is compromised.

Your patients and the people you interact with will probably be very upset if they find out that their information has been compromised and that they weren't told.

But, of course, it's a voluntary scheme. So, at the moment, the situation is that there's no requirement to notify.

**DR JULIAN WALTER:** I've pulled some data off the OAIC website. In 2015-16 there were some notifications made, 107 of them all up. Health was the third largest notifier, but the numbers are not enormous - 107 notifications across Australia, across many areas that are subject to the legislation.

It's worth noting that in the Health sphere there is both State and Commonwealth legislation. The State legislation will generally apply to public hospitals. The Commonwealth legislation will apply to private practice and also to private hospitals. What you are seeing here isn't a subset of notifications from all of the health providers.

Surprisingly enough, Health is only third worst, but we'll have a bit of a look at that.

Moving on to next year. Thursday 22, February, is there any reason it's Thursday?

**MR ANNAN BOAG:** That's a very good question; not one that I've turned my mind to. I don't think there is.

**DR JULIAN WALTER:** I think the anniversary of when the legislation passed, I suspect that's the reason; that or as a *Hitchhiker's Guide to the Galaxy* fan, "it must be Thursday".

**MR ANNAN BOAG:** 22 February is a very big day; I think it's probably the first day that I'm going to see a notifiable data breach for the first time based on how many we might get. It's probably the first day that one will happen.

22 February is when the scheme comes into force. Any breach that occurs on or after 22 February needs to be notified. So, it's not about when you find out, it's about when the breach occurred and that's the day when this all comes into effect. Start thinking about these issues now, if you haven't already.

**DR JULIAN WALTER:** Why is Health important?

**MR ANNAN BOAG:** We identified a few different sectors that we're trying to focus on to get messages out about the scheme to help people understand that it's coming into force and what they need to do, and Health is one of those sectors. There are a few reasons for that.

One is the sensitivity of the information that healthcare providers obviously hold; it doesn't get much more sensitive than people's medical records.

A second issue is that the scheme generally applies to businesses that have a turnover of more than $3 million but in the Health sector, all businesses, if they're one person, two people or a private hospital, are covered. There are a

lot of people who might have obligations under this scheme, so we've got to think about how we can reach them.

One point that you made to me when we were speaking about this earlier, was that the nature of medicine is that there's personal information being frequently shared between people, so that may also increase the chance of a breach occurring.

**DR JULIAN WALTER:** Walid, in your practice, what sort of information resources do you put into privacy?

**DR WALID JAMMAL:** Right now, as much as I need to and by February it will be a lot more. From a practice owner's perspective, definitely we have already started telling people it's time, the time has come - it's already a requirement obviously with the Privacy Act, but in terms of the IT security and the practices' policies, procedures and protocols around it, the time has come to spend money on it, certainly to turn your mind to it to make it more than just a tick box in the accreditation process in general practice and I can only speak in general practice.

At the moment, it is an accreditation process that we go through and many bits of it are nothing but a tick box exercise. But the time has come where it is going to matter, it is going to really matter from the privacy law respect.

**DR JULIAN WALTER:** Alison, we've spent the last many years educating doctors and practices that they needed to have a privacy policy, I think we've probably got that message through now to most of the doctors, but the new message that we're having to communicate is the data breach response plan. Are you advising anyone about data breach response plans at all?

**MS ALISON CHOY FLANNIGAN:** Yes, absolutely. I've been advising our clients to ensure that they've got a data breach response plan in place, because now's the time to plan it, so that if there is a data breach, then they know what to do before the legislation starts, and start to train their staff.

In addition, I've been advising clients to review their contracts with contractors, particularly IT contractors who might hold information on behalf of their organisation, as an agent of the organisation, so that if you're renewing the contracts for contractors, that there is an appropriate data breach notification clause in that contract. It's all in preparation.

**DR JULIAN WALTER:** Do the privacy policies need updating?

**MS ALISON CHOY FLANNIGAN:** I think they should be updated to be compliant with the law. Certainly, it depends on whether you update them now and go through a voluntary scheme now or whether you update them and get them ready for when the legislation starts, but certainly the expectation is that you should always keep your privacy policy up to date in accordance with the legislation.

**DR JULIAN WALTER:** It's worth noting, as the slide says, it's not mandatory to have a data breach response plan, so this is basically the plan that says who does what, who rings who, what are you going to do if you have one, who's your IT person, who are you going to contact, what are you going to do with your systems? It's fantastic to have it ready but it's not a mandatory requirement. It's obviously going to be very useful if you have a problem. Annan, do you have anything to say?

**MR ANNAN BOAG:** I'd say that any time is a good time to review your privacy practices and check whether you have an updated compliance privacy policy. We did an assessment of 40 different GP practices a few years back. Out of the 40, I think 36 were able to produce a document which was called a Privacy Policy on request. Whether they existed before we made the request is another question for you, but we took that at face value.

Of those 36, 20 referred to the Australian Privacy Principles, the rest referred to either the National Privacy Principles or some other legislation or didn't talk about the legislation at all.

When we looked through the requirements of APP1, there is a list of things that need to be included in a privacy policy. I think four policies had all of the requirements.

When you are getting ready for the scheme, one thing to do would be to check you have a privacy policy and that it talks about the APPs and that it meets the requirements that are set out in the Act.

**DR WALID JAMMAL:** It is interesting you are saying that about general practices. That captures probably what's happening out there now, in that we've had for years part of the accreditation process, the fact you need to have a privacy policy but the accreditors actually don't check that the policy complies with the Australian Privacy Principles, so no one actually sits down and reads it line by line.

I think this is another message that we really need to get out there, as I've said before, the time has come but in every medical business, not just general practice, IT, privacy and security around the IT is now everyone's business in terms of everyone in the business.

**DR JULIAN WALTER:** Particularly with the exposure on 22 February next year when your privacy breaches are going to come to the attention of the Office of the Australian Information Commissioner, so there may be a little bit more scope to look at what has been prepared as a privacy policy and similar documents.

I thought we might start with the scenario now. Walid's working in his practice, he turns up early this Thursday morning, 22 February next year and he goes to log on to his computer and it looks like this. We're going to simplify the scenario somewhat, so I appreciate there will be some complexities and IT issues that may not reflect what actually happens just to make the discussions a bit simpler tonight.

Walid finds that he's got this message on all of his computers, his phone, his smart watch and basically what it is saying is that his practice files have been encrypted by an external third party, so, a hacker. That third party will decrypt them for money, so bitcoin in this case, $300 worth, probably US dollars in this particular scenario. If he doesn't pay that money, he's got three days and the amount will go up. Then if he doesn't pay the raised amount, what will happen on 28 February is that his entire file system will be deleted.

In this circumstance, and probably realistically, the hackers haven't got access to the actual content of his servers, they've just got access to the files which they have locked out. So, the data that he has on his database is still encrypted using his own protection that would have been built in by the software provider. He still has his passwords for all of his staff to login.

The hackers can't actually at the moment get access to the patient records, but they can certainly cause inconvenience to Walid. Tell me Walid, what is your day like when you've just turned up and found that this has happened.

**DR WALID JAMMAL:** I did write down a few four-letter words, but I crossed those out and came out with a five letter word and that's "awful" - and a few other words. This is, certainly from a GP's perspective, as a practice owner or a

practitioner, a nightmare. It's a nightmare irrespective of whose files got stolen or looked into or not.

The business is at a standstill. If you think we can still see patients and we'll function, I'll tell a story of a time when my actual server did go down, not to this, it just crashed, and one of my registrars said, "Oh my Lord, we need to go home, I can't see patients". I said, "Yes you can" - make up her name - Emily. "We don't know what's happening but we'll try and get it fixed."

She said, "But how do I write a prescription?". I said "Pen, paper". She went, "I don't even know my prescriber number. How do I do that?" I said, "Use my script pad." "I don't have a script pad." "Use my script pad, you cross out my name and just write yours."

That's the sort of dependency that we have obviously to computers and general practice more so than any other parts of the profession. We've been computerised for many, many years.

This can and will bring the business of our practice to an almost standstill.

**DR JULIAN WALTER:** Presumably you can't book new patients in, because that's electronic, you can't contact patients because that's electronic, you can't store records, because that's electronic.

**DR WALID JAMMAL:** Our entire data base links into an online appointment system, the phones would run hot. We don't know who's coming, who's going, pathology results, x-ray results, you name it, everything depends on that, both the computer system and the internet actually.

**DR JULIAN WALTER:** This WannaCry virus or hacking tool that's been used is real, it was used in a whole lot of breaches earlier this year and it has brought various health practices and other businesses to their knees around the world, so, it is a very real event.

**MR ANNAN BOAG:** Probably given the scale of this particular attack, there'd be some people in this room who would have seen this screen on a device that they owned. In the first 24 hours that this virus was travelling around the world, it infected 240,000 different systems. It was massive.

These kinds of attacks are on the increase. They are a privacy issue because they involve the unauthorised

modification of data, but fortunately, this attack and a lot like it, aren't a data breach notification issue, because although the information has been made inaccessible, the attacker hasn't downloaded it. They haven't got it themselves and there isn't a risk that they'll publish it, but something that is scary is that some attackers might realise that that's something that businesses will want to avoid and will be willing to pay a lot of money to avoid.

Maybe we'll start seeing attacks that do threaten to disclose data as well as just encrypt it.

**DR JULIAN WALTER:** In this scenario Walid is prepared, he has a data breach notification plan, he pulls it out and the first thing he has is "Get out the Nokia phone". The Nokia phone is going to work, it hasn't been hacked and now he can start ringing some people. Luckily, he has on his piece of paper the number of a couple of people. Who are you going to call, Walid?

**DR WALID JAMMAL:** You, Julian. Actually, Alison, that's who I'm going to call, call my lawyer, call my IT guy, call my bank and make sure they've cleared money for cash payments as soon as possible.

**DR JULIAN WALTER:** And your practice manager.

**DR WALID JAMMAL:** She's already there because I married her.

**DR JULIAN WALTER:** The fact that you have had an incursion at your practice, is this a breach of the Australian Privacy Principles, Alison?

**MS ALISON CHOY FLANNIGAN:** There's an obligation under the Australian Privacy Principles to use reasonable measures to ensure that data is secure. It's not automatically a breach of the Australian Privacy Principles. You need to look at what Walid's done in terms of the security of the systems and the report on Pound Road Medical Centre actually provides some good indication of how high a standard the Commission requires, in terms of security, obviously more than putting three padlocks on a shed.

But certainly, if he's put in reasonable security measures, then just because someone has hacked into his system doesn't mean that it is a breach of the Australian Privacy Principles, but then going forward, once that's happened and this legislation commences, then it will very much depend on how he responds to that.

**DR JULIAN WALTER:** It's worth noting, just for those people who are sitting there terrified by what has happened, the other places that you can contact - and I won't go into any detail about this - but there is the Australian Cyber Crime Online Reporting Network. They, reassuringly say on their website, that if you contact them, they won't contact you back.

There is also the Australian Signals Directorate, which provides some useful guidelines in terms of things you can do to minimise the risk. They have these top four techniques that will reduce 85 per cent of the adversary techniques used in targeted cyber intrusions.

That's a lecture for another day but if people want to go to those sites and have a look, they can.

In this particular matter, we know there's been an IT breach of the systems. In responding to this, the OAIC suggests that we work through a number of steps - our response to the intrusion.

The first thing is, obviously contain it; that's going to be an IT issue, your IT guy is going to disconnect our network from the outside world I presume and then they're going to do IT magic to it, and you're going to sit down and work out what's happened.

Walid's already given us a bit of an idea. The IT person is able to tell us that it appears that the files themselves have not been accessed or are accessible, but the files and system can't be used.

In terms of the risks associated with the breach, again we've addressed that. In this case it's probably more of a business risk rather than a privacy breach per se.

I guess the question is, while you're getting all of this information, what sort of notification are you going to put up? Initially, Walid, what are you going to do? Your practice isn't working.

**DR WALID JAMMAL:** Put up signs, tell people we've got a computer problem, a big one and try and get our head around the damage caused both to the network and also trying to assess the privacy of the data base.

**DR JULIAN WALTER:** Would there be an expectation that the practice had to go into any detail at this stage, or is

putting up a notice saying “There was a computer outage, sorry, the practice isn’t working today”, reasonable?

**MR ANNAN BOAG:** If this was a breach that had to be notified under the scheme next year, there would be some extra things that you needed to say, which we’ll probably get to later on.

**DR JULIAN WALTER:** This is early on though.

**MR ANNAN BOAG:** It’s not something that we would regulate, that relationship you have with the customer, it’s common sense. What do you think that they’ll want to know and what do you want to tell them. There’s no particular requirement as part of the Privacy Act, of what you tell people at that stage.

**DR JULIAN WALTER:** In this case, obviously thinking about preventing future breaches will occur in time, and again, it’s going to be mainly IT related information. For this first matter, for every medical practitioner who owns a practice it’s their worst nightmare in terms of an event. Is ultimately notification required? I think we’ve got the answer to that - the answer is probably “no” in this very simple scenario, although it’s obviously going to depend a lot on the circumstances of the hack. Any thoughts about that? Is there agreement, we’re not going to notify this?

**MS ALISON CHOY FLANNIGAN:** Because this scenario has the assumption that the actual data has remained intact and hasn’t been disclosed, but in real life what we would do, the first thing we would do is ask your IT people and if they can’t answer it, ask an IT expert whether this particular virus has the capability of accessing your data, and if it does, then you go through the next step. If the data is intact, then arguably it’s not a notifiable breach.

**DR JULIAN WALTER:** Which came as a bit of a surprise to me, but having worked through it all, it makes sense.

The other thought that crossed my mind, Walid, the $300, would you pay to have your system decrypted?

**DR WALID JAMMAL:** Yes. Does that answer your question?

**DR JULIAN WALTER:** Any thoughts from the OAIC?

**MR ANNAN BOAG:** There are not great figures out there about this, but there is research that’s been done by a few different security vendors who put out a range of different

figures, and I've seen anything from around 30 per cent to 60 per cent of people who are affected by attacks like this pay, which surprised me; that's higher than I would have expected.

It's generally advisable, as the privacy regulator, I would say you should not pay because if you pay, what you're signalling to this person who has attacked you and compromised you, that you're willing to pay if they do it to you again, and also the fact that there are a lot of people out there who are willing to pay, means that there's a market for this sort of thing to happen.

If we all stop paying, it would stop, but I appreciate the reality that you're in, it's a tough decision to make.

**DR JULIAN WALTER:** There is some work that's been done by IBM on this. This came out last year. Firstly, they noted that spam emails with malware were very, very common, so an increase of 6,000 per cent in 2016 and I guess that's because hackers have found a business model.

In terms of what happens when that information is hacked, so they've noted it's incredibly lucrative and that cyber criminals in the 2016 year were on track to make nearly $1 billion out of this - so, incredibly lucrative.

More importantly, they also looked at who would pay and perhaps unsurprisingly, businesses were more prepared to pay, so 70 per cent of executives who were a victim of a ransomware attack would be prepared to pay. Obviously, cost is a big issue. For consumers, it would be 50 per cent or so, although those who had photos hacked were more likely to pay.

**DR WALID JAMMAL:** It depends on the photos.

**DR JULIAN WALTER:** Indeed, because you could have already been scarred by the Ashley Madison hack. The other issue was price and again, it's not really relevant to us tonight but there's obviously a cost at which it becomes something that you're not going to pay even if you were contemplating it.

A lot of these hacks are for very low amounts of money, which is why they were successful.

There was 50 per cent of those executives that had been hacked paid over $10,000 and 20 per cent paid over $40,000.

That gives you some idea of the cost to disruption of business that the hackers are playing with.

**MS ALISON CHOY FLANNIGAN:** Can I add something?

**DR JULIAN WALTER:** Yes, of course.

**MS ALISON CHOY FLANNIGAN:** I recently presented at our own seminar and I presented with a cyber security expert, so I thought I'd just share some of his tips, which come from the government website that you referred to in terms of trying to secure your IT, which I thought would be useful for you to know.

The number one tip he told me was to make sure that you are up to date with your software. Quite often you have software and they come with patches and updates. The software companies keep an eye on what viruses come out. Make sure your IT department, as soon as that update or patch comes out, they put it on and don't delay.

The companies that were affected by that big breach were the ones that weren't up to date with patches; so that's a big thing.

The other thing is also making sure that you have policies and procedures, a lot of it's to do with human error, so policies and procedures about telling your staff not to open suspect attachments and that's what you just talked about. It's about ensuring that if you're not sure about it, don't open it. Those are some of the useful tips that I learnt from that cyber security expert.

**DR JULIAN WALTER:** We thought we might move it to a more disclosable breach. Now the practice manager has taken the backup hard drive home and although the system is well encrypted, the backup hard drive is not. The data base is not encrypted and there are records on there, for example, emails that might contain documents that are easy to access.

The hard drive is sitting in the back of the car and she comes back from wherever she's gone, the car's been broken into and the hard drive is gone. On that hard drive, there's potentially up to 20,000 records.

Now we've got a slightly different scenario, where we don't know where the hard drive has gone. It probably isn't targeted, in the sense that it's not an attempt to sabotage the practice data and it may very well be that the hard drive

is just going to be wiped and sold, but we're not entirely certain of where it might end up.

The way we work through this in terms of assessment is going to be a little bit different. Alison, we contact you for advice, what are you going to say about this breach?

**MS ALISON CHOY FLANNIGAN:** The first thing we do is we refer to the legislation and the section has two components. There must be an unauthorised access to or an unauthorised disclosure of the information - clearly that has occurred.

The second thing is a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

Although it's a current guideline, they will review it when the legislation commences, the Office of the Australian Information Commissioner has published a useful guide - Data Breach Notification Guide - A Guide to Handling Personal Information Security Breaches. I do commend that to you.

Clearly, there has been a loss of information and because of the sensitivity of the information, in my view it's got a medium to high chance that it would be something that would cause, because it's got medical records on it, serious harm to any of the individuals involved.

You would start doing an investigation. The legislation does talk about certain things that you would look at to see if there is an eligible data breach. For example, who has access to the information, the nature of the information, whether it's been encrypted, etcetera. If it hasn't been encrypted, as you said, then you'd be seriously considering that that particular scenario is an eligible data breach.

**DR JULIAN WALTER:** In this case it may well be a mix of both health information and patient's private information - their date of birth, their name, their address and potentially also financial information, their credit card details, other data, so Medicare card numbers, although you seem to be able to get them off the Dark Web anyway these days with not much trouble.

In this case you've got quite a serious issue. If we are going to make some sort of notification to the patients, given that there are an awful lot of patients, what are we going to do?

**MS ALISON CHOY FLANNIGAN:** Is that a question to me?

**DR JULIAN WALTER:** Either Alison or Annan. Alison, how would you draft it? If I'm ringing you and saying I need to tell my patients that we've just had a breach. Are you going to tell everybody straight away?

**MS ALISON CHOY FLANNIGAN:** I would do an assessment of trying to find out as much information as possible, what information was on the device, find out who's actually affected, find out what potentially happened to the device. Do the sort of investigation that you would normally do and then from that I would draft a potential notification and in doing the notification be very careful that you don't breach other people's privacy.

There are certain things that the legislation does require quite a quick review of. You have to review within 30 days and assess all the things that are in the legislation. I think the Red Cross handled - I don't know whether you agree with me - it quite well in terms of doing a notification to--

**DR JULIAN WALTER:** We'll come to that in just a minute; I've got some quotes from them.

**MS ALISON CHOY FLANNIGAN:** Certainly, you can say, we've had a data breach issue. If you've got any concerns please contact us. Here's the contact name. You notify them in the form that you normally communicate with them, so, if you communicate with patients via email, what I usually do, encourage clients from day 1 to put in a procedure where you make sure that the breach is not going to occur again.

This is the one that's left in a car isn't it, but certainly if there was a system issue, you would be making sure that you secure the information as soon as possible, you put in policies and procedures to ensure it doesn't occur again.

There are certain communications that you can make to make the public feel comfortable that even though the data breach occurred, that procedures have been put in place to make sure it doesn't occur again.

**DR JULIAN WALTER:** Can you apologise?

**MS ALISON CHOY FLANNIGAN:** Absolutely.

**DR JULIAN WALTER:** We're probably going to have an apology, we are going to talk about the data that was lost. What

about telling the patients that the OAIC is involved, Annan, is that required? It may not, of course, occur at this point in time.

**MR ANNAN BOAG:** It's not required. It can be a helpful thing to say but in a lot of breach notifications that I see where it's also been reported to our office, that's generally something that people would tell the individuals who've been affected.

Can I just step back with this scenario to one of the points that Alison made, which was that at the start of this process before jumping in to notify, you should be doing an assessment about what the situation is, because to me this is not a black and white absolutely we must notify case.

One of the objectives of the way that the legislation was written was to not cause over-notification, so people getting notifications every day, every week don't pay any attention to them. We only want people to be notified of breaches where there's a likely risk of serious harm.

The legislation sets out a whole bunch of factors that you need to think about when you're deciding whether there's a likely risk of serious harm, the type of information that is involved, it's sensitivity, whether it's protected, encrypted or not, and in this case a lot of the factors would seem to point towards notification, but ultimately the question is whether it's likely that any of these 20,000 patients will suffer harm.

If, in your investigation you can determine that the reason this was stolen was to wipe and sell the device, if you get advice from the police that that's almost certainly what occurred, then quite possibly it wouldn't be a breach that you'd need to notify.

I'd say don't rush right in and tell the 20,000 people and the OAIC, you've got at least a few days to try to figure exactly what's happened here and evaluate whether there's a serious risk to the people and whether notification should occur.

I feel like I've gone off on a bit of a tangent and not actually answered your question.

**DR JULIAN WALTER:** No, that's very appropriate, that's very relevant.

**MS ALISON CHOY FLANNIGAN:** The difficulty for us is that the legislation hasn't commenced and it's not until you get the cases that you'll have more guidance as to what to notify and what not to notify.

**DR JULIAN WALTER:** And it will be very interesting to see whether what we think tonight is actually what occurs in the real world after February 22 next year.

**MR ANNAN BOAG:** When you are sitting on the fence, remember that the vast majority of people in the community think that they should be notified if their information is compromised, regardless of this legal change of whether there's a likely risk of serious harm or not.

You may go ahead even if you think that there's not an absolute obligation to notify.

**DR JULIAN WALTER:** Is there any plan from the OAIC in terms of what view they take towards these notifications earlier on, i.e. are we planning to be in an educating mode or if there are accidental breaches, is it likely it's punitive? Do we have any sense of that?

**MR ANNAN BOAG:** Our focus at first will absolutely be on educating and on assisting people to comply with the scheme. If we come across occasions where we think people have wilfully avoided obligations under it, then that will be a different matter.

But the objective at first would be to help people come into compliance. If you did, in this scenario, decide that there wasn't a likely risk of harm, I'd suggest you should really have a solid basis for that conclusion and write down what it was, so that if we are asking you down the track what that reason was, you could answer it in a sensible way.

**MS ALISON CHOY FLANNIGAN:** When are we getting the updated guidelines?

**MR ANNAN BOAG:** As soon as possible. We put out some draft resources on our website. You can get to all of them at oaic.gov.au/ndb - for notifiable data breach.

One of the documents is about identifying a notifiable breach and it walks through the process of deciding whether a breach is in or outside the scope of the scheme.

**DR JULIAN WALTER:** There'll be a link to that from the slides here if anyone gets access to them.

**MR ANNAN BOAG:** Before the end of this year is the goal.

**DR JULIAN WALTER:** The other information there may be about what you're going to do about similar breaches in the future and I guess that's preventing the harm to other people. Similar to medical adverse events, where patients want to know even if you can't fix the problem that they have, that the same problem is not going to happen to someone else; so, a useful step.

Also, I think it's worthwhile making sure that you have some sort of consistent message at your practice, someone for them to contact if they want to get more information. That person is certainly going to be busy with a breach of this magnitude if you're notifying everybody.

**DR WALID JAMMAL:** I'm going to suggest it's the practice manager who lost the drive.

In preparing for this talk, on the Sunday night I had the pleasure - because I had nothing better to do than writing up a policy on passwords, disc handling, chain of custody for my receptionists who take home my entire data base every night as a backup. They emailed me back saying yes, agreed, signed and that's what we're going to do.

**DR JULIAN WALTER:** The other thing is that if you have any recommendations for patients about what they need to do or what they need to watch out for, again, that's information that you can include in this notification to the patients that's been made.

In terms of notifying the Office of the Australian Information Commissioner, Annan, can you give us an idea of how quickly we do this? Is there a timeframe that you want this information in?

**MR ANNAN BOAG:** At the point that you've decided that the breach is one that you have to notify about, then you need to notify both us, the OAIC, and the individuals who are affected as soon as practicable. I can't tell you how many days that is, but the task of notifying us, it should be very quick. We're going to put up an online form that you can fill out to tell us.

If you need to contact a large number of people through a variety of different mechanisms, that is something that might happen over the course of a few days rather than immediately, but it should be done as soon as you can.

**DR JULIAN WALTER:** As the guidelines suggest, the information you are going to include on this notification, keeping in mind you're probably getting some assistance with this anyway, but who your organisation is, because obviously the OAIC doesn't know who you are, a description of what happened, what sort of information was involved, which obviously relevant to tonight is going to be health information mostly, and recommendations that you provided to the persons whose data has been breached. Is there anything else you want?

**MR ANNAN BOAG:** That's the minimum information that you need to provide to individuals and to the OAIC. We're going to be putting out a bit of a guide about some additional information that we'd like to receive voluntarily so that we can understand the breach and whether there's anything that we need to do in response to it.

In terms of the notifications to the individuals, I really say that you should just treat that as a minimum requirement for what should go in that notification. If you look at organisations that did really good breach notifications, the Red Cross is one of those that we'll be talking about soon, you'll see, if you go to the website that they set up to do their notification process- I work in complaints handling and I've seen so many disputes fall down when there's an agreement that a matter will be resolved on the basis of an apology and then the apology says, "I refer to our discussion, as agreed, I undertake to offer you my sincere regret that this incident occurred."

There are very bad apologies out there, but the Red Cross, they gave a great one in their notification, so I think that should be part of the notification, you should try to speak to your patients or to your customers in the voice that you want them to hear you in.

**DR JULIAN WALTER:** I think we've got an example up there. I don't know whether this is a spoken apology by the head of the Red Cross or whether that's actually what they sent out, but it's very heartfelt. "We are extremely sorry, we are deeply disappointed to have put our donors in this position".

Why the Red Cross information mattered particularly, so it wasn't necessarily that they revealed your ABO blood group, but one of the questions the Red Cross asks if you're going to donate is whether you have engaged in any high risk sexual activity recently. So, that information was contained in the breach. I don't know whether there was other

particularly sensitive information, but that alone would be enough potentially to allow people to be blackmailed, and incredibly sensitive.

I understand in the Red Cross breach that the notification came from someone who discovered it and the information potentially wasn't spread very wide at the time.

**MR ANNAN BOAG:** That's the case, they contained the breach. They were fortunate enough that the person who discovered that the information was online was a bit of a good Samaritan and decided to do the right thing and report it to them.

I think in the immediate days following the breach there were real questions about how many people might have accessed it and who might have seen it. Nonetheless, they quickly determined that it had been accessed a very low number of times and they tracked back to who the accesses were by and identified that it was a discrete set of people who they could check had destroyed the information and not disclosed it further.

But nonetheless, they still went ahead with this notification process.

**DR JULIAN WALTER:** Here there are some techniques which you can pick up; they had messages sent out to their clients by SMS, it contained simple information but also gave them a site to go to for more information. I don't know whether the original site changed as time has gone on, it probably has. Currently that's an excerpt from what is available online at that site if you look at it now, but I presume that they gave running updates during the matter.

**MR ANNAN BOAG:** Part of what they did so well as a breach response was keeping people really informed about everything they were doing and all the information that they had about the breach, as they went through the process. We got very few complaints about this incident, considering how many people were affected, we received less than a dozen individual complaints from people in the community who were unhappy with the disclosure information.

I'd say if you're going to look at an example of an organisation's very good breach response, look at the Blood Service.

**DR JULIAN WALTER:** And they got the gold star as well in terms of the summary of the event, the Commissioner sang great

praise of the way it was handled. Again, these are excerpts from it. “It was very reassuring to see what they did”.

One of the issues is even if there is a breach, what we call an eligible data breach, it may be that you can do things about that breach that mean that the risk is removed or at least reduced to a point where it doesn’t need to be notified anymore.

We thought we might work through some scenarios of simple breaches. These are email breaches where information has gone to the wrong place, and probably in the real world these are far more common, they happen every day. I’m sure most of you who’ve used email have done this on occasion.

One of the questions that came in was about the use of email and I just thought rather than spending a lot of time on this, I’d put up a couple of points.

The RACGP talks about the fact that you should be aware of the fact that all communication methods are inherently unsecure and email is also insecure. You should be making sure, if you are sending information by email, particularly health information, that the people you are sending it to appreciate that, particularly patients.

It’s not prohibited per se. We certainly see with AHPRA sending us material, they encrypt patient records now, perhaps not some of the other surrounding documents. They didn’t always used to do that, but that’s a more recent development and the OAIC also has - and I won’t go into this in great detail - some advice on email security and other things that you should at least consider, whether you can improve the security of the communication. Did you want to say anything or are you happy?

**MR ANNAN BOAG:** I think that covered it off. Email is not, you shouldn’t consider it to be a secure communication but by the same token, I don’t think it’s a whole lot less secure than sending something by post.

We don't think that just because you send something by email it’s a breach of the Privacy Act, but encryption is something you should consider, when sending, certainly large volumes of sensitive information.

**DR JULIAN WALTER:** The other issue which again we had some questions about, and I won’t go into it in great detail tonight, but is sending material overseas. The Privacy Act does deal with that.

It’s beyond the scope of what we’re talking about tonight, but there are requirements. If you’re sending data across a border in terms of what you need to do to make sure that that is handled appropriately and again, if you need to find out some information about that, either speak to your MDO or look it up online; the information is there, but we would run out of time to cover that tonight.

In this circumstance, our patient is a 15-year-old girl. She’s come to the practice. She has had a consultation about symptoms which suggest she has an STD. She has testing done and she says to the practice “Look, I want my results sent back to me by email”. So, that’s what occurs.

The first issue, again is a question that we were asked, what is the situation with this 15-year-old girl in terms of access to her records, can she control them?

There are some guidelines out there that discuss this. Again, it’s a topic in itself, but the OAIC guidelines talk about the fact that with an under 18-year-old it will be a case by case basis, but there’s a general presumption that, obviously it would still be assessed on a case by case basis, that someone aged 15 or over has the capacity to consent to what happens to their records.

That would fit in with what we consider as Gillick competency. In other words, a person’s ability to consent to their healthcare goes hand in hand with their ability to control what happens to their records. That must be the case, otherwise their parents could potentially just ask for the records after the consultation.

Again, the general rule here, that an individual under 15 is presumed not to have capacity, again, on a case by case basis.

You can see that this is not entirely consistent across government services, again, it’s case by case, it doesn’t really matter. My Health Record presumes that from when you turn 14 you’ve got capacity to make decisions about your My Health Record and with Medicare, you can get a Medicare card from the time you turn 15.

But it gives us some idea; this 15-year-old girl, she is Gillick competent, she does have the ability to control where her records go. She has requested for this information to come back to her by email and that’s where the mistakes occur.

Walid, do you get many patients wanting information by email?

**DR WALID JAMMAL:** Increasingly so, absolutely, it's the way of the world. In fact, what I see it as is part of the service that we provide.

In this particular circumstance, clearly, we're not going to rush in and just send it without specific patient consent and specific patient request. With this STD result being the result that it is, I'd probably want to talk to the young girl first, have a discussion with her and if she really wants the result to be transmitted by email, then that's what we're going to do.

We've got a process in place to make sure that we send it to the right person, that we identify her, we send it to the right person. There are many different processes out there. We've got what I call a practice protocol, and I use the word "protocol" because every staff member has to follow it step by step by step - there are no shortcuts.

**DR JULIAN WALTER:** In this case, the protocol is about to breakdown for reasons unknown. In the first instance, the email gets sent to another GP, this is not a GP treating this patient, it's a random GP that's somehow got a similar name to your patient. How are we going to work through this? Annan, do you want to give us an idea?

**MR ANNAN BOAG:** When we're looking at whether a breach is a notifiable one, we'd say that it's really a three-step process, there are three things you should think about. Firstly, has there been a data breach, has there been unauthorised access or disclosure of personal information? Secondly, is there likely to be serious harm to the person whose information is involved? Thirdly, can you do something to reduce that harm, such that it no longer exists?

This is a case which illustrates the importance of really understanding the breach and trying to respond to it very quickly, because I think you can probably do something here to minimise the harm to the person involved. You've disclosed it to a GP, they're in your inbox already, you probably know them and have a relationship with them, so I suspect you can probably get on the phone to them pretty quickly, explain to them the situation and get them to destroy the email.

I think it would probably be a reasonable assumption for you to make that that person would do so, knowing that they have their own professional obligations, because you have this

relationship with them, I think it would be quite safe to conclude that if they told you that they'd destroyed the information, they in fact have. In that case, there wouldn't be a continuing risk of harm to this individual.

If you have any doubts about that, you may well want to notify her and let her know this has occurred. In fact, you might just want to do it anyway, as a matter of courtesy. I think the majority of people understand that emails sometimes go awry and if you told them quickly that that had happened and that you'd done something to fix it, it probably wouldn't be a huge problem for you.

But if you were considering whether this is a notifiable breach, I'd say that if you take the right steps and remove the risk, it's probably not.

**DR JULIAN WALTER:** The data breach gets a bit more complex, if instead of sending it to another GP, you send it to the mother but in this case, the mother sent the daughter in for the consultation, so she knew what the daughter's symptoms were and there's obviously a good relationship between mother and daughter in this circumstance. Alison, how are you going to work through this?

**MS ALISON CHOY FLANNIGAN:** I think you've partially answered the question, you would have to work as a team whether there is an implied consent by the daughter that the mother is to know information about her records, and that can be done by the conduct. So, clearly, if the mother came into the consultation with the daughter, that would be an indication that the daughter has consented, implied consent that the mother can have that information.

You would have to assess that and then if there's been consent, obviously there's been consent, so there's been no breach. But, you'd need to actually ascertain the circumstances of the relationship between the mother and daughter and whether you can say that the daughter has consented to the mother having the information.

**DR JULIAN WALTER:** Walid, in this matter what step are you going to take first up after you've become aware of this. All you know is that the email has gone to mum, you're not really sure whether mum knows or not, so what are you going to do?

**DR WALID JAMMAL:** I'm going to call the daughter.

**DR JULIAN WALTER:** And have a discussion. That discussion goes well, although she's somewhat upset that the wrong email was picked, but you talked to her, mum already knows, and as we've worked through, you're probably not going to notify this matter either because the harm has been minimised or eliminated potentially.

**DR WALID JAMMAL:** To me as the practice owner, this represents basically a break in that protocol, in that step of double checking, at least double checking where the email is going.

Actually, this happened in not quite the same circumstances but it nearly happened, it was a near-miss in my practice yesterday.

**DR JULIAN WALTER:** As the breach gets worse and worse, this time the email has gone to mum but she's unaware of the consultation, so, in this case the daughter really didn't want that information to go. Presumably the same step is going to occur, we're going to contact the daughter and see what happens, but potentially she makes a complaint about it to the practice, so clearly, she's unhappy about it.

She might make a complaint elsewhere, to the healthcare complaint body in your local area or other places. Are we going to notify this matter, do we think it likely? It's going to depend a lot on the circumstances, Annan, do you think this is a notifiable matter?

**MR ANNAN BOAG:** It's tricky. There are a few complicating factors here. It sort of sounds like in the scenario that the breach might have come to your attention because the daughter has told you or she's complained to you about it.

If that's the case, you might ask what's the point in notifying her? However, if you do decide that there is a risk of serious harm to her, then notification to the OAIC will be required and you may also need to notify her of anything in the notification statement that she hasn't already been told about. It's the sort of matter that you could work through the steps in the legislation, look at the resources that we've put out, any policies that you might have about how to respond to a data breach and make a call one way or the other about whether notification should occur.

**DR JULIAN WALTER:** You've got time to work through those issues I understand, it's not a matter that you need to decide straight away. It might be after a week or so the daughter has become more accepting of it or the practice has

responded and apologised. Do you still have to notify if you consider that you've addressed the issue?

**MR ANNAN BOAG:** That's a possibility, if the harm can be remedied, if you can speak to the daughter and the mother and somehow resolve this situation, then you may still choose to notify the OAIC if the legislation applies but I'm probably not going to be very interested in it.

What are your thoughts on this one, Alison? Have you thought about how the legislation would apply in this case?

**MS ALISON CHOY FLANNIGAN:** I think it will really rely upon the reaction of the daughter when you ring her is the answer, and I agree with you that if she feels that she's not suffered harm, then you've remedied it and therefore it becomes not notifiable.

But if she is very upset about it, then she knows about it, there's a process to go through with the legislation.

**DR WALID JAMMAL:** In terms of the harm, I think the key is going to be the relationship between the doctor and the daughter and the mother and the family. I think we can't go past that human relationship in terms of assessing the risk of harm.

**DR JULIAN WALTER:** If we flip the scenario, so now the data that is sent out is much less sensitive, so maybe the daughter has just been in for a cold and she's been told she's got a viral illness, she's not been prescribed antibiotics, she's been sent on her way with Panadol and all those things that we do these days.

The actual breach of information that's been sent to the mother is not great, but in this case the daughter, for whatever reason, is particularly sensitive to her information being sent to the wrong place.

Can the mere fact that there's been a breach cause harm or is it always related to the actual privacy that is breached?

**MR ANNAN BOAG:** It's really dependent on the particular person and the circumstances that sit around them. Whether a breach is notifiable or not is an objective test, it's about what a reasonable person would conclude in your circumstance when they're looking at what's happened, but if you're aware that this patient might react in a very big way to what a lot of people would consider to be a very minor disclosure - and I'm sure there are people who you work with who would react

in a big way over something that most people would find quite small.

If you're aware that this particular individual's circumstances would cause them to suffer subjective serious harm, then yes, it is a breach. It is a risk of serious harm to that person so you may need to notify, but if you didn't know that about this patient, if you think that they're not going to have a big reaction to this, then it may well not be a notifiable breach.

Again, it's one of those borderline cases. What would the patient expect? Probably want to know that you've emailed this information to her mother, whether it's about her cold or an STD, so I'd say you probably should tell her, but whether it's a notifiable breach will depend on her particular circumstances.

**DR JULIAN WALTER:** Just to give some idea in our final example of some of the complexities involved in trying to find out what is going to occur. If you've sent the email to an unknown third party, you don't necessarily even know whether they're in Australia, but in this case, we'll presume that they are and you contact that third party and say this has been sent in error. They say, yes, I will delete it.

What are we going to do in terms of being sure that they have? How do we satisfy ourselves? Is there anything we can do in deciding to report or not to report? How satisfied do we have to be? Can we rely on what they've said to us? Annan, any thoughts about that?

**MR ANNAN BOAG:** This is very different to the situation where you've disclosed to another doctor. If it's a random email address, you have no idea who this person is, you probably can't put much weight on what they're telling you. I'd probably suggest in this scenario you should err on the side of disclosure, if you've got no way of verifying where this information has gone or who might have received it.

But, work through the steps in the legislation, ask your advisors if you're really struggling to come to a conclusion one way or the other and make a reasonable call.

**DR JULIAN WALTER:** Does the OAIC have any power over the third party if they're in Australia?

**MR ANNAN BOAG:** We might if they're a business with a turnover of more than $3 million or if they're a health service

provider, but if it's a random email address, then the odds are that they're probably not.

We do sometimes contact people who've received information in the course of a data breach and request that they destroy or delete it or not further disseminate it and we do have some success in getting those kinds of undertakings formally, but whether we've got powers to take them to Court and make them not disclose the information, well, in this scenario you've got an email address, how do we even find the person?

I don't think we're going to be able to solve this problem for you, most likely.

**DR JULIAN WALTER:** That brings us to the end of the presentation.

**MR ANNAN BOAG:** On a depressing note, sorry.

**DR JULIAN WALTER:** If there are any questions that anyone has, you're welcome to ask now or alternatively, you can come up to any of us that are staying afterwards and have a talk about these issues or other privacy issues.

There were certainly some other questions that we just didn't have the time to cover. I've got some of my own questions that we didn't have time to cover either, which we'll follow up as well. Any questions for anyone before we close the night?

**QUESTION:** Thank you very much, very helpful discussion. I just wanted to clarify the issue about disclosure to the 20,000 patients, what would be reasonably required as part of the disclosure, particularly given that some of these practices will be sole practitioners and will not have the resources to contact individually 20,000 people?

Would it be sufficient in that situation to put a notification on your website, or is there an expectation that you are going to have to contact them individually?

**MR ANNAN BOAG:** There are three options in the legislation for notification. The first and I think the default option, is that you contact everyone directly. You can choose which mechanism you want to use, but generally it should be a way that you usually contact them.

The second option is that you contact only those people who are at risk of harm. In this scenario, if you have some way of grouping the people who are involved in a data breach

into those who are likely to suffer serious harm, say those that have had their full medical file disclosed, versus those that have only had their contact details disclosed, you only need to tell those people who are in serious harm.

The third option, if it's not practicable to contact people directly, is to publish a notification on your website and take steps to draw people's attention to it.

It generally wouldn't be enough to just put the notice on your website, you're going to have to take some steps to draw it to the attention of the people who are affected, so, perhaps you'll tell them when they come in for consultations that this has happened or put a sign up in your practice or find some other way to draw it to their attention.

I'm not sure that just the cost of writing to 20,000 people or contacting 20,000 people would necessarily push something over into that not practicable territory.

We're looking, at the moment, at telling a large number of people about a data breach that has occurred and looking at the costs around sending out text messages to all of them; it's a few hundred dollars to send some several thousand text messages out. It's not free but it's not an enormous cost.

**DR JULIAN WALTER:** Presumably you also have to be careful that you don't breach the privacy of people in sending out that information, if they're old contacts for example.

**MR ANNAN BOAG:** We actually think probably the scenario where it won't be practical to contact everyone is more often if you don't have their contact details rather than it's going to be too expensive to send them a letter.

**DR JULIAN WALTER:** There is a lot of scope for sorting that out when we come across more of these whole scale health data breaches, where the practice data base may not be that up to date in terms of patients who've moved. Would it be acceptable to pick some sort of rational number and go back two years' worth of patients and let them know and then have a message online and in your practice for the others?

**MR ANNAN BOAG:** I hadn't thought about that scenario, it's an interesting idea. You don't necessarily need to notify everyone at once. The requirements to notify people is as soon as practicable, so there are people who you know you have got current contact details for, you've got their email addresses, you can probably contact them, then the people

that you're not so sure about you might only have a postal address.

If you don't have current contact details and you don't have any straight forward way to get them, then that's probably a situation where you should be considering a notice rather than writing to every individual.

**DR JULIAN WALTER:** Or you don't know whether their details are current, which is probably more the issue.

**DR WALID JAMMAL:** This is a problem that we're going to face, and hopefully it's not going to be me, my practice, because it is terrifying actually as a GP. In my practice, I've got 11,000 files that are open and another 9,000 that are closed. By closed, that means they haven't been for three years and I've got files, electronically, that go back to 1994, when I put my first computer on my desk. I don't want this to happen.

**MR ANNAN BOAG:** If there is doubt about the accuracy of the contact details that you have, yes, it's probably not going to be practical. Though, one way that organisations address this in data breaches that I have seen, the notifications that they send out say to text messages, to mobile phones, they're quite brief, they don't go into any details about the particular person's circumstances.

They'll provide a link to the more detailed statement that appears on the website, but once again, it would be written in a way such that it won't compromise anyone's privacy if the wrong person reads it.

**DR JULIAN WALTER:** We might draw that to a close, but as I said, you're welcome to come up afterwards and ask us questions if you've got them. Thank you very much for your attendance.

MEETING CONCLUDED