Electronic Health Records

Leanne O'Shannessy graduated BA LLB from Sydney University and was admitted as a solicitor in 1985. She is currently the Acting General Counsel for the New South Wales Department of Health, as well as their Acting Director of Legal and Legislation. Prior to joining the Department's Legal Branch, Leanne held positions in the NSW Law Reform Commission and Cabinet Office.

Her current role as Acting Director, Legal and Legislation, and General Counsel includes primary responsibility for NSW Health's legal services and the legislative program for the Health portfolio.

I have been asked to talk about the legal implications of Electronic Health Records. This is an awfully amorphous, large and vague subject. As many of you would be aware, the legal implications of EHRs have been contentious for some years and will, I think, continue to be subject to contentious debate as they come on line.

Dr Dalley's presentation was interesting, including the comments he made towards the end of his talk as to whether or not this is, in fact, the best way to spend our money. From the perspective of government and a health care system looking for solutions to a range of problems we now face, I suspect that EHR will continue to be pursued. Nevertheless, his comment is very important and reminds us of the need to assess and review systems for value for money.

The Special Commission of Inquiry

It is worth noting that, at this very moment, NSW has a Special Commission of Inquiry looking into acute hospital services in NSW. It is important to recognise that this inquiry was called as a result of the outcome of an inquest into the death of a patient in the Northern Sydney Central Coast Area Health Service. Three issues identified in that inquest are crucial to the Special Commission, being run by Peter Garling SC.

Two of those issues concerned the supervision of clinical staff and communication between health professionals. The last relates to clinical note-keeping and record-keeping. This is an area of crucial concern. It is very likely that EHR will be a key issue as we progress through the inquiry.

I think it is also worth mentioning the perspective I bring to this issue, as a lawyer employed by the Department of Health. In that role, I have been assisting and advising people who are trying to develop EHR. So my perspective is very much a legal policy view of the sorts of issues that come up and the sorts of issues that need to be grappled with when developing an EHR.

I am not going to be able to offer you solutions tonight, because many areas of development of EHR are still fluid. The future has to do, not only with a legal perspective, but also with changing community attitudes.

Health e-Link

Dr Dalley mentioned Health e-Link, a record system linking a range of systems. It is being piloted, as a summary record only, in the Hunter and in Western Sydney. I think that this distinction – summary versus a complete record - is important. From a legal perspective, different issues will arise with an electronic record system to which everyone has access and into which they contribute data, as opposed to a system which is simply a summary of events.

The Electronic Medical Record

The other system being developed at the moment in NSW Health is the Electronic Medical Record (EMR). Having an EHR and an EMR is a little confusing. The EMR is basically an Area Health Service-based system, and is thus confined to the public system. Dr Dalley also mentioned HealthConnect, which will provide a national health record and which has changed considerably as it has been developed.

Legal issues

The view has often been put that, from both the legal and community perspectives, EHRs are contentious and difficult, and that we have to find new and completely different ways of dealing with the subject. It is important, however, first, to go back to where we started.

The health system has, for many years, collected information, used information and regulated when it allows that information to be disclosed. In relation to medicine in general, common law duties of confidentiality have applied to the use of information for many years.

So it is not so much a matter of asking, "What do we need to re-do?" It is a matter of looking at what an EHR actually does and, from a legal perspective, asking what is different about EHR? What about it requires a new way of looking at how we do things? The first issue is privacy.

Privacy law in general

The issues with privacy are twofold. When introducing an EHR, you have to think how you can make it work under our current privacy laws. The second thing, because we do get to make legislation in this state, is to ask the policy question: if we have some capacity to control what those privacy laws say, how they should apply?.

Depending on the design of a system, issues of liability and potential liability might also arise.

When we discuss EHR, we need to understand what is meant by 'privacy'. The NSW Health Records and Information Privacy Act, the main state-based law affecting health records, both in the public and private sectors, embraces fifteen Health Privacy Principles (or "HPPs"). These HPPs operate as a kind of cradle-to-grave regulation of information, applying from the time you collect it, hold it, use it, and store it – until you have to dispose of it.

Collecting information

A number of principles deal with collecting information (HPPs 1-4). You can only collect health information if you have a lawful purpose, and the collection must occur with minimal intrusion. The information generally needs to be collected from the person to whom it relates, provided that it is both reasonable and practicable to do so. There is a recognition that, very often, information can appropriately, and must appropriately, be collected from third parties. The collection HPPs also provide that certain information should be given to a patient when you are collecting the data. The information required to be given to a patient concerns what the provider is going to do with the data, whom they will disclose it to and how they are likely to use it in future.

Keeping information

There are also general provisions on how long you should keep information (HPP 5), ie only as long as 'reasonably necessary' for the purpose it was collected for. There are also other obligations on how long you are required to retain it. For example, the public sector has obligations under the State Records Act (1988), obliging it to keep records for certain periods of time.

Security of data

The security provisions (also HPP 5), on which I will talk further, are quite simple. The information must be subject to such security safeguards as are 'reasonable in the circumstances'. Frankly, I think that, if there is one crucial issue with privacy law and EHR, it is the question of security.

Access and alteration

There are also provisions for access and alteration (HPPs 6-8). Basically, people need to be able to know if you have information about them. They need to be able to gain access to that information and, if they consider it it is inaccurate (HPP 9), to request an agency to alter it.

Use and disclosure

In a general talk on privacy, I would probably spend most of my time discussing use and disclosure, because 90% of privacy issues relate to disclosure (HPPs 10 and 11). The issues, in relation to written records or an EHR, are the circumstances in which it is appropriate to disclose information and are generally much the same in relation to both paper and electronic records. One would expect the same rules to apply.

Other provisions

Provisions in both the NSW law and the Federal Privacy Act relate to the use of identifiers (HPP 12). Primarily, they restrict the use by non-public sector people of a public sector identifier. There are provisions allowing people to obtain access to health services anonymously (HPP 13). However

NSW law has a *caveat* which states that services can be obtained anonymously only where it is both lawful and practical to do so'. In many circumstances, people are required to provide their name, for example in relation to Medicare benefits.

There are also provisions about taking information outside NSW (HPPs 14): ensuring that you either have consent or that there is an equivalent applicable privacy law or scheme in the jurisdiction to which the information is being taken.

Then there is what I call the NSW 'special'; a privacy principle that exists in NSW only – specifically directed at the linkage of records. This is HPP 15, which is directed at EHR systems which link identifying health records.

Privacy issues and EHRs: laws are paper-based, EHRs are not

The first really big issue in trying to make privacy issues and EHR work together - and it sounds a bit odd but really is quite a big issue - is the fact that all the privacy laws, in all states and federally, are paper-based. An EHR, by definition, is not paper-based. This raises a number of issues.

'Silos' of information-laden paper

Our privacy laws are based on the premise that there are separate and distinct 'silos' of information which can be regulated. Dr Dalley also used this term, which I consider particularly apt. In some ways, the privacy laws reinforce the concept of silos.

The silo, in this case, is the agency or organisation or medical practice holding the information. Because the law is paper-based, it treats information as a physical thing which can be moved between silos. The use and disclosure provisions of privacy law then work by regulating or restricting or controlling the way that the 'physical' information is moved around from silo to silo.

This works fine when you have a paper-based record system, but e-health doesn't work like that. When you design systems, you will have information zapping around servers which might well be within different agencies. A lot of these 'disclosures' simply authenticate that what you are putting into the system is correct or confirm the identity of a person who has been entered.

There can be no or very limited possibility of human access to this information as it moves around all these computer systems. But there is still a very strong possibility that, technically speaking, there is a breach of the law because it is moving around these systems. It is a bit like the Buddhist question about a tree falling in a forest where no-one is there to hear it – does it make a noise? In EHR the question is, if no-one can access it, should it be considered a disclosure? If nobody is actually going to be able to access it – no human being, that is – is it a breach of privacy?

Although I don't have an answer, I do know that, while the wheels appear to grind slowly at the federal level, there has been considerable thought given to how you can try to adapt these paper-based laws to make them user-friendly in an e-environment.

Fragmented laws

The second issue is that the law is fragmented: we have many privacy laws across the country. In NSW, the Privacy and Personal Information Protection Act (1998) applies only to the public sector and to general personal information. We also have a Health Records and Information Privacy Act (2002), with the HPPs, which applies to health information in both the public and private sectors. The Federal Privacy Act (1988) has ten National Privacy Principles (NPPs), which apply to the private sector and to private sector health care providers, but not to the public sector. Some time ago, we also released a draft National Health Privacy Code, which, I hate to tell you, has things called NHPPs – National Health Privacy Principles.

Anybody who has worked in privacy will know that there is a huge industry in arguing how complex and confusing all these laws are – how the world will end because there are different laws with a lot of people making money out of encouraging this! The truth, generally speaking, is that while there is some confusion (I have had to give advice on three different laws on the same issue), they are, by and large, operationally very similar. The broad content of what they say is generally very similar.

Where I think there is a real argument for consistency and uniformity – for having one national standard – is in the electronic environment. Electronic systems are going to be national: they will need clear guidelines for what they will do, across the whole country.

Opting in or opting out

The other big issue with privacy and EHR is, "Are they opt-in or opt-out?" With the opt-in model, unless you expressly consent for your information to be a part of this record, you are not in it. With the opt-out model, unless you expressly refuse, your information is included.

Basically, with an ordinary paper-based record created in a hospital or GP practice, patients don't really get much say in whether or not a record is created. The record is owned by the practitioner or by the health care system; it is a way of obtaining and recording information in order to provide appropriate care. You don't get a choice about whether or not you want the record to be created or whether or not you want to be involved in its creation.

The reason we argue so strongly about opting in and opting out is not so much the fact of our information being recorded, but the fear of the range of consequences which can arise with an e-health record which will not arise in a paper-based record system.

The debate on opting in and opting out is moving. In 2000, when we prepared the Health Records and Information Privacy Act, passed by Parliament in 2002, it included Health Privacy Principle 15, which requires that linked systems be opt-in. As a result, while the general privacy rules apply to all records, there are special rules for electronically linked systems. There is still a very strong view at the Commonwealth level, and amongst privacy advocates and privacy commissioners around the country, that e-systems should be opt-in.

From an operational point of view, however, there is probably increasing discomfort with that approach. The Health e-Link trial, for example, has been given an exemption from HPP 15 to trial working as an opt-out model. The opt-out model operates by providing patients with a substantial amount of information when they are first enrolled, and is designed to make it as easy as possible for them to opt out if they don't want to be included. The Health eLink trial is ongoing and is being evaluated. That evaluation will guide whether or not it continues and whether or not it continues as an opt-out scheme.

Dr Dalley also mentioned the trial in Hobart. I understand that one of the reasons why NSW decided to pursue an 'opt out' model was the amount of time it was taking to enrol patients and to obtain consent in the Tasmanian pilot.

Security of Information and e-systems – HPP 5

As I mentioned earlier in my talk, security of information in e-systems is an ongoing cause of public concern. With a paper-based system, there is a physically finite capacity to breach privacy and to obtain information: disclosures and breaches are a matter of physical movement of, or access to, a tangible record.

With EHR, however the potential for a breach and the volume of information which can be affected by a breach is extraordinary. The size of the error might be very small, but the outcome extremely serious. While privacy laws just say that security should be 'reasonable for the circumstances', we are in a bit of a green field site about what would be considered 'reasonable' in any particular case. When you have privacy laws, as in our State, which provide for judicial review of decisions, allow for the payment of impose compensation and the imposition of fines on agencies which don't comply, it creates an issue which needs to be considered seriously.

Two examples show that we shouldn't be worried so much about hackers and disgruntled employees, as about straightforward, basic human error.

A breach affecting 25 million people

The first example will, I think, be recalled by many people as it occurred quite recently in the UK. In November 2007, Her Majesty's Revenue Service lost some child benefit data. The data included names and addresses, date of birth and bank and building society account details.

What happened was this: the Revenue Service needed to send the data to the United Kingdom National Audit Office as part of an investigation being done by the NAO. A junior officer copied the data onto a disc. The disc was not encrypted. The disc was sent out through the standard post but never reached the NAO. It contained details of 25 million British citizens, 7.5 million families. It created a storm in the community and in the media. I understand that, to date, the information has yet been retrieved.

The point of this story is that it wasn't a hacker or a disgruntled employee who intentionally breached privacy. A number of questions arise. How did a junior officer have access to that data?. How did they copy it? It shouldn't have been able to be copied without all sorts of rules coming into play. It was copied unencrypted. It was sent through the general post. There was a series of errors and thoughtlessness – just human error.

A breach affecting one individual

The second incident, which occurred some time ago, again demonstrates how simple human error can be a problem. A transgender patient also had mental illness and other issues. This person was a regular attendee at the emergency department (ED) of a local hospital. To assist with their care, a special ED plan was devised. It was to be available in the ED's electronic system 24/7, so that whoever was on duty whenever that patient came in, could have access and know the best way to treat the patient.

The person responsible for updating and uploading the plan on the ED system was a clinician - not an IT specialist. The clinician went into the system to save this plan into the ED folder, but accidentally put it in the wrong folder in the server. The material went into the area health service's Intranet and was then uploaded to the area health service public Internet. Just an error in saving a document into the wrong folder.

It was taken down as soon as the area health service found out, but the patient had found out from someone they knew, who had contacted them to say that their information was up on the Internet.

In the first case in the UK the breadth of the breach was extraordinary. In the second case, the personal cost to one person was extraordinary.

Education and human error are issues in all we do in the health care system. Then we get into the issues such as overwork and clinicians doing administrative tasks and it all compounds. It is an area which history has shown to be have some of our biggest problems.

Control of access

Another area which will be a growing concern in future relates to access and control of content. In NSW and some other jurisdictions, the EHR is promoted as something which gives individuals control and rights over their information held in the system. Often this will mean that they have automatic access to everything which is on-line. In a paper-based system, access has to be gained through the hospital or the clinician, who will decide if access is granted. Patients have rights of access under the privacy laws, but there are also provisions which restrict their access, particularly if that access will place someone else at risk.

As public sector lawyers, we deal with child protection issues, with mental health patients and with others who, when unwell, can be dangerous and threatening. In child protection cases, family members sometimes threaten staff who are involved in care or reporting of suspected abuse. It is crucial in these circumstances, where there is a high risk, that there is some capacity to control patients' access. This is difficult when you have an open-ended access system for patients.

Control of content

A second concern is control of content – or to put it more correctly, the patient's capacity to control access to the content of their record. One of the big debates, as the systems are being designed in NSW, is whether or not a patient should be able to determine who – that is which particular clinicians or hospitals – may or may not have access to their record. For example, a patient may say "I don't want that hospital to see my records". Or "I don't really like that doctor – the specialist was rude and unpleasant, and I really don't want to have anything to do with them".

The patient might have legitimate reasons for this concern – particularly if the information is of a personal and sensitive nature - but on the other hand, if the record starts to get increasingly fragmented, it becomes unreliable. Clinicians might then become reluctant to use it because they will be concerned about these limitations. There are ways of addressing this issue: warnings to people and the like, but this is an area policy-makers need to watch carefully in future.

Legal liability

Finally, I will just mention the question of liability. It is early days and we are just starting to consider these issues. On one level, what Dr Dalley said about the surveys was interesting: that, whether or not you have an electronic system, the quality of the outcome doesn't seem to vary that much. Where I think EHR could be a great boon for the lawyers, who may come to these issues some years after the event, is when they are trying (1) to find the record, (2) to read the record, (3) to see who had gained access to the record and when, and (4) who signed off on it. They are going to be in heaven.

Some NSW hospitals do have EHRs and have had them for a long time. Some of you might have had dealings with those hospitals. These records can be clearer and more reliable than the paper based variety: easier to show who was involved in care, who signed off and all of those types of issues. This brings me back to the current Special Commission of Inquiry: this issue of clarity of records and the availability of records is going to be crucial – and this is an area where EHRs can show a really positive improvement.

The liability issue which is, I think, potentially more of a problem from a legal perspective is likely to relate to the reliability of the content. As I mentioned earlier, when referring to patient access and control, one of the concerns is that if this control means that clinicians – or certain clinicians – are allowed access only to bits and pieces of the whole picture, and they, in turn, are making judgments on such limited information, it creates a minefield when you later come back and try to determine if the practitioner knew a particularly important or crucial piece of information at a particular time and try to trace through when that information was available and when it wasn't. It opens up the possibility of contradictory arguments from the patient about when they gave people access and when they didn't.