Wigley & Company

BARRISTERS and SOLICITORS

ELECTRONIC HEALTH RECORDS
Legal Issues

28 June 2004

The NZ Electronic Health Records Summit
Auckland

P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833
also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

Electronic health records are an important issue in the health sector. Wigley & Company spoke at the NZ Electronic Health Records Summit in Auckland both in 2003 and 2004 and this paper deals with the EHR risks and solutions.

EHRs carry legal, privacy, and other risks. But they bring huge benefits which should not be held back by those risks. Trying 100% to meet legal and other risks would make EHRs unworkable. The idea is to get the benefits and minimise the risk.

We'll start by reality checking some of the issues because it's important to put legal and other risks in context. We turn then to the Electronic Transactions Act and its implications for EHRs.

Next up are industry standards and specific health issues, such as on-line prescriptions and passing EHRs to third parties (eg: hospital to GP; DHB making NZHIS information available to GPs via its own network, and so on). We'll touch on EHR policies.

EHRs offer great benefits, yet come with legal, privacy and other risks. Those risks can't be eliminated. Benefit and risk need to be balanced, and the barriers to reduce the risk shouldn't be set too high. The risk shouldn't be ignored. Rather it should be confronted.

INDEX

1 OVERVIEW

1.1 EHRs carry legal, privacy, and other risks. But they bring huge benefits which should not be held back by those risks. Trying 100% to meet legal

and other risks would make EHRs unworkable. The idea is to get the benefits and minimise the risk.

1.2 We'll start by reality checking some of the issues because it's important to put legal and other risks in context. We turn then to the Electronic Transactions Act and its implications for EHRs.

1.3 Next up are industry standards and specific health issues, such as on-line prescriptions and passing EHRs to third parties (eg: hospital to GP; DHB making NZHIS information available to GPs via its own network, and so on). We'll touch on EHR policies.

2 REALITY CHECK: FOUR INTRODUCTORY POINTS

2.1 **There's a balance**: First when we talk about legal risks, we're including privacy risk. Legal risk is of course only part of the story. There are other risks such as security, difficulty of accessing information if barriers are set too high (such as in emergency situations), the very real risk of ministerial or senior manager angst, and "Auckland Herald front page" risk.

2.2 But the potential benefits are much more important. It's no exaggeration to say that the benefits of EHRs are massive. Multi-million dollar gains are to be had. Efficiencies are greatly improved. Lives are saved and improved. It's easy for the lawyers, privacy specialists, and security experts etc to point to barriers and hold up progress. But nothing should get in the way of progress down the electronic health communication path, and robust 24x7 availability of information where needed. There needs to be a balanced and holistic approach which gets the benefits and minimises the risks. Legal issues can't be addressed in isolation. It is better to confront the issues, try and find a solution, or elect to take the risk, having minimised it.

2.3 **Benchmarking against the current situation**: The current mixture of paper and electronic records is inherently risky. Faxes, for example, carry far more risk of undesired disclosure than unencrypted emails. Overall, the risk is less in the electronic environment than the paper based environment.

2.4 **Electronic solutions are not perfect**: Even the most stringent methods of protecting EHRs have real weaknesses. Surprisingly, this issue is often not confronted when the risk and benefits of PKI and digital certificates are addressed. PKI is the most robust practically available methodology to, using the language in this area, *authenticate* (ie: confirm who is sending and receiving the EHR), preserve *confidentiality*, preserve *integrity* of the "document", and to provide evidence that the sender is bound by what he or she is saying (*non-repudiation*). Structured well, this is a highly robust system.

2.5 But a big weakness is that digital certificates can be and are misused. The great thing about signed paper records is that it is almost always easy to work out whether the document and the signature are genuine or forged.

That level of certainty can't currently be achieved with digital certificates (let alone any other technology on the horizon such as biometrics). The digital certificate is typically loaded on a Microsoft-based platform. It might have modest protection (eg: a password screen saver). But, in real life, it can often be readily used by others in offices. Not only that, but others are often encouraged to use an individual's digital certificate. That can happen in practice even if the individual has signed a policy document confirming he or she alone will use the certificate. Of course, there can be other types of internal misuse, and risk of external hacking, leading to compromised authentication. Many smaller health providers operate in exposed security environments.

2.6 Take an example. Say ACC contractually bind GPs to be the only people that can send in electronic claim details (AC 45s). In practice many GPs are going to delegate some or that entire role to administrative staff. No amount of legal mumbo-jumbo is going to stop that. If there is a fraud (where ACC or the Police need to prove the case beyond reasonable doubt (a very high level or proof)), can the lodging of claims by the doctor be proved? Depending on the circumstances, the prosecution may have to show that a particular person "signed" the claim. They may struggle.

2.7 A much lower level of proof than the criminal level applies to many other types of legal claims and disputes (including privacy enquiries by the Privacy Commissioner and the Health and Disabilities Commissioner). In many cases, the level of proof is often "on the balance of probabilities". That requires the party trying to prove the point to show that a fact (eg: that the GP was the person who "signed" the electronic form by sending it personally) is more likely than not to be the case. Proving a case is easier in those situations. It is harder with a criminal scenario. Yet how often do health sector agencies consider those types of issues? Prosecutions and other court and tribunal issues are not mainstream considerations for EHRs, but they are considerations nonetheless.

2.8 Of course the event of electronically lodging of claims, in the example given above, is not the only evidence that ACC or the Police could rely upon. In most situations, there is a lot of surrounding evidence. There could be an extended history and the pattern proves the point. Or all the evidence put together brings things home to the culprit. But that doesn't get around the point that this is a difficult area and the best way forward needs to be considered. That's so especially for those who have a compliance issue (eg: funders where there could be fraud). In the latter case, look a lot more closely at evidential issues, including the inadequacies in this area due to delayed introduction of a new Evidence Code, which is not met by the introduction of the Electronic Transactions Act.

2.9 Of course potential prosecutions are only side issues to the main aim of EHRs. Ultimately, setting up a system to catch the crooks may erode the key EHR drivers. It may make things too expensive. So it's best to cut some corners to achieve primary outcomes.

2.10 We come back to an earlier point. We may be worse off because, for example, one or two fraud cases can't be proven or because there's some breach of privacy obligations. And so on. But far more important is the ultimate goal of improving health services overall. Nothing should stand in the way of that. The idea is to minimise the risk overall, in practical terms.

2.11 In any event, chasing fraud, checking for privacy and security breaches, and so on, in paper records has its own problems. Many of these problems are solved with EHRs. For example, one of the great things about the electronic records is that it is much easier to audit and monitor what's going on. Say for example forgery is suspected. While easier to prove in a paper-based world (where's there is handwriting), it is far easier to audit this in an electronic world, to see patterns, systemic abuse, etc. Paper records can only be sampled randomly (nothing more than a small fraction of a percent could be checked). Electronic records can of course readily be checked on a much bigger scale. We deal with electronic prescriptions below as an example of this.

2.12 There is some good material on the downside of PKI (and, by inference, the downside of other authentication methodologies such as PIN numbers, etc). A great source of material and cross-references is Roger Clarke and his numerous articles on the Australian National University and Xamax Consultancy websites. Material such as this is worth reading to get a skeptic's view on PKI, to help decide the best way forward, based on realistic assessments of risk.

2.13 Ironically, by the way, an argument can be mounted that using simple user name and PIN numbers might sometimes be more reliable as a way of identifying and authenticating individuals than so-called stronger digital certificates. It's more likely an individual will keep a PIN number in his or her head, and not load it on a computer where it can be misused. But digital certificates must be kept on a computer and can be hacked, read and used by others, and so on. Risk is minimised by use of tokens, smart cards etc, but the risk with digital certificates remains. And of course internationally there's been very slow pick-up of PKI, many PKI projects have failed, and it is an unwieldy process. There's differing views for example on Australia's Gatekeeper process, under which health sector PKI such as HESA-based solutions reside. For a scathing attack see Roger Clarke's submissions to the current Joint Parliamentary Audit and Compliance Select Committee hearing. But you'll see that there are views to the contrary, including those of people from HESA.

2.14 We are not saying that a PIN approach is preferable, nor that PKI is unsuitable. Rather, there are options to consider.

2.15 Of course new technologies will increasingly reduce the risk, although none yet comes near being 100% reliable, particularly as to authentication. For example, biometric methodologies still carry risk and the possibility of misuse. For confidentiality, non-repudiation, and integrity, however, currently available technologies and methodologies are amply acceptable.

2.16 **Privacy Requirements:** Importantly, the privacy legislation allows that balancing. Key in this area is Rule 5 of the Health Information Privacy Code. This requires health information to be protected to a level that is reasonable in the circumstances. Of course EHRs generally attract high-level security requirements in relative terms.

2.17 Note however that much health information is less sensitive or can be made less sensitive by taking out some information that's not required for the circumstances. While an agency may decide to maintain robust protection for everything, on a KIS basis, information availability and protection can be categorised and handled according to sensitivity (in practice that'll happen anyway). In this paper however we'll focus on inherently sensitive material. But it's important to look at options for less sensitive information (eg: unencrypted email, provided it's done within strict parameters, is acceptable, often desirable, and often safer than the alternatives in the paper and fax world, although note the restrictions in the NZ Standards material, noted below).

2.18 Coming back to Rule 5, we've got highly sensitive information, to be protected to a level "reasonable in the circumstances". Those "circumstances" shouldn't just include having high barriers to protect the information. Importantly, they should include ready access to information to enable better health outcomes and efficiencies. The barriers must not be set so high such that lives are lost because information can't be obtained in emergencies. Health providers need to have practical access to information on a relatively quick basis (perhaps with emergency overrides available). Those are significant points which should dilute the countervailing desire to maintain high-level security and privacy protection. 100% privacy and security protection is not the optimal outcome if clinical and efficiency goals are to be achieved.

3 ELECTRONIC TRANSACTIONS ACT

3.1 **When does it apply?** While enacted last year,[1] it won't be in force until later this year. That's because some regulations need to be passed first. They deal with issues such as Credit Contracts and tax records.

3.2 **Overall approach of the ETA**: There is an international trend away from technology specific legislation (such as legislation based on a PKI model). The trend is toward technology-neutral legislation. This has happened for example in England, Australia and the United States.

3.3 The new Act doesn't mandate specific technology. Rather, it tries to put electronic and paper worlds on a largely equal footing.

3.4 **What does the Act do?** The ETA boils down to three key parts. First it says that electronic information is not denied legal effect solely because it

[1] To see the Act, go to www.legislation.govt.nz and click on the link to the Electronics Transaction Act.

is electronic.[2] There is nothing new in this. The Courts are generally great at responding to new technology developments. Generally they will enforce something that is electronic just as much as if it is paper based.

3.5 **The quality of the electronic evidence is key:** The big point here is that, whether something electronic works from a legal perspective is usually a question of the ***quality*** of the evidence. Take the example above of an ACC claim. In theory the electronic evidence (the digital certificate based on the PKI model) is the most practically robust authentication method. But evidentially, it will not always be possible to prove that the person saying they "signed" did in fact "sign".

3.6 Often this point about the quality of electronic evidence is overlooked. A click accept on a webpage does not necessarily link the acceptance of the particular terms to a particular individual. If I install new Microsoft software on my computer, I don't click accept the Microsoft license terms. Our computer services firm does that, and their click accept doesn't bind me to the terms. More to the point, Microsoft could have difficulty proving, if I deny click-accepting, that it was me that did it. Say a DHB employee click accepts an online policy. The DHB might struggle later to prove he personally did this, so that he's bound by the policy terms. What happens when he brings a personal grievance because he is dismissed for looking at porn on-line in breach of the online policy? Or an administrator looks at Helen Clark's health records in breach of a click-accepted policy?

3.7 For this reason, online policies, security and privacy policies, and other staff manuals and procedures relating to security and privacy, should have *hand signed* acknowledgement from the employee, contractor or other third party. (See however the alternative noted below). Online acknowledgement is too risky with current technology. Its fine (actually desirable) to have the policy residing electronically. All that is needed is a document which is signed by the employee and which very clearly links that signature to the on-line policy, and identifies key and onerous obligations. Note however that it's particularly important to get the form right from a legal perspective. A high percentage of forms like this fail to work. This is a big risk area.

3.8 A good example for the health sector is IRD's approach to authenticating on-line tax returns and the problems Peter Gutmann says that IRD face as a result. See www.cs.auckland.ac.nz/~pgut001/pubs/ird.html.

3.9 Sometimes buy-in to policies and terms don't matter so much. So online click accept is OK from a risk point of view. After all, getting individual signatures to a document can be unwieldy and has inherent problems anyway, such as messed-up documentation, failing to keep the signed document, and so on. Indeed, those risks are so great in practice that, on balance, an organization, even with key policy and contract requirements,

[2] Section 8, Electronic Transactions Act

may decide to do things on-line. This should be a calculated risk (often it's not).

3.10 A good example of low risk for on-line buy-in is Amazon's when it sells books from Amazon.com. Amazon's risk in selling books is extremely low and so there is no need to get something signed up. But Boeing's risk on selling a $10 bolt for a 747 is extremely high. Boeing must not sell that bolt (even though it is only worth $10) without getting a signature in writing from Air New Zealand which includes a contractual limitation on liability. Similar risk assessment concerns apply in this sector.

3.11 **Second part of the ETA:** The next part of the Act[3] sets out some default rules for when and where information is deemed to be received and sent. This could have some practical implications depending on what the health sector agency is doing, but generally that would not be the case.

3.12 **The main focus of the ETA:** Then comes the third aspect, which makes up most of the Act. Here's the big point. It only applies to what are called "legal requirements". These are defined as requirements in Acts, Regulations, etc.[4]

3.13 Acts or regulations do not directly cover many things that happen in the business and health sector. For example, most contracts have little to do with Acts and much more to do with judge made law (such as offer and acceptance etc). Therefore in most instances something like a contract is unaffected by the main part of the ETA. This is the same with many transactions, records etc in the health sector. Their creation and use is often not driven directly by acts or regulations. So the ETA makes little or no difference.

3.14 Other Acts and Regulations: Other Acts and regulations can have effect anyway, overriding or supplementing the ETA. Take for example the Health (Retention of Health Information) Regulations. They confirm that health information can be kept in any form (implicitly that includes electronic form), with an issue of course being whether the EHRs are accessible over the 10-year period in view of changing technology etc (Regulation 6 and 9).

3.15 **What if there is a "legal requirement"?** The ETA contains various rules that enable transactions, documents etc which had to be paper based to be handled electronically (and vice versa). There are rules about "signing" electronically what would otherwise be paper documents. Coming back to the point above about quality of evidence, the required strength of the signature depends on the circumstances. For example a web site click accept may be enough, and sometimes a digital certificate may not be enough because of its uncertainties as noted above (there is a default provision to define the perfect signature but, arguably, even PKI doesn't met its needs). Covered is means of giving access and providing

[3] Sections 9-13
[4] Section 15(2) Electronic Transactions Act

information electronically. And rules cover electronic retention of documents. Note that, generally, doing something electronic which is currently paper based requires agreement to that approach from sender and recipient.

3.16 We are focusing on EHRs but records, which are important to many health sector agencies, are tax records. They often have to be retained for 7 years. Under the new regulations, tax documents that are paper based (such as paper tax invoices) can only be retained in ***scanned*** electronic form. But this is a special case and other retention methods elsewhere will be acceptable.

3.17 Take the invoice for example. A paper based invoice typically consists of (a) a form which does not change from invoice to invoice (eg: the supplier's logo, address, GST number etc) and (b) fields which change from invoice to invoice (details of services provided, price etc). The information that changes of course resides in the supplier's normal computer accounting records. But the new regulations confirm that it is not enough to just retain that information. A scanned copy of the actual hard copy invoice is required. The reason is that the tax department wants better evidence than the basic electronic records. Ideally it would want the original paper for forensic purposes. They are compromising by accepting a scanned version of the original.

4 HEALTH SECTOR EXCLUSIONS UNDER THE ETA

4.1 A number of Acts and Regulations are excluded from the ETA.[5] Quite a few of the exclusions are from the health sector, but most are for isolated documents which would typically remain anyway in paper based form, such as notices under professional bodies legislation (eg: the Medical Practitioners Act), mental health compulsory assessment notices, and so on.

4.2 **On-line prescriptions:** The key exclusion of a pivotal health document is the prescription. The Medicines Regulations[6] require prescriptions to be hand signed by the practitioner. If it wasn't for the exclusion of this part of the regulations, prescriptions could now be done electronically. This is the right call for a start. Until the issues are worked through, prescriptions should still be hand signed.

4.3 There are of course huge potential benefits for the sector from enabling electronic prescriptions. Take a private sector example: the GP hand-signs a prescription. This is unwieldy even though it's increasingly done on a PMS system, so there are electronic moves already. The patient takes the prescription to the chemist, who re-keys the information (with of course risk of error and adverse patient outcome). Then there are further procedures in the Healthpac claims process, etc. There are obvious advantages in making this seamlessly electronic.

---

[5] See the Schedule to the Electronic Transactions Act
[6] Regulations 41 and 42

4.4 Until recently, we thought the risk of electronic prescriptions would be too high, given the risk of misuse and forgery, and the inherent authentication problems even with PKI. We thought we would have to wait until better technology came along than, say, PKI based authentication.

4.5 However, a comparison with paper prescriptions suggests we're at the point where on-line prescriptions are an acceptable risk. Hand based prescriptions are inherently prone to risk. In practice, auditing and monitoring (eg: for forgery) is difficult except on a very limited basis.

4.6 An advantage of electronic prescriptions is that much systemic misuse can be detected by electronic auditing. Any misuse, except on an isolated basis, should be detectable. Of course the benefits of introducing electronic prescriptions are huge (and outweigh in my view the disadvantages).

4.7 Of course, risk can be minimised. For example, the law could still require hand signing of the prescriptions for particularly risky drugs (eg: narcotics). But even then it may be better to have prescriptions made electronic. There will be questions about how best to authenticate (eg: whether PKI is required). These issues can be worked through. My own view is that the sector can move to electronic prescriptions, looking at things from a legal perspective. Maybe there are wider issues to consider?

4.8 By the way, we are not sure we would exclude certain drugs such as narcotics. There's a good example where, maybe, imposing additional restrictions has a reverse effect (as may happen if, for example, narcotics require hand signed prescriptions). Take the ACC. Health providers are able to electronically batch-process AC 45 forms. But certain types of claims which are perceived to be sensitive must still be done in the traditional way. An example is the area of claims based on sexual abuse. Practitioners will mail or fax these into ACC. That is a far riskier process than sending them in electronically, even if the information was sent unencrypted by email (We are not suggesting that happens; rather we are illustrating relative risks).[7]

5 WHAT EHRS ARE COVERED BY THE ETA?

5.1 Set out in the appendix are some examples of affected legislation, with indications about what and whether agencies can and should do. If it's

[7] There are of course issues around unencrypted emails, which in practical terms can and should be used in the health sector with strict rules and guidelines to cover privacy and security issues, and minimization of risk. Note however the encryption requirements in the Health Records Standard. Risks in relation to transmission across the internet are low (and acceptable in my view for much correspondence), with regard however to the key risk area of a mailbox hosted by an ISP which can be hacked (or read by an ISP staff member). The rest of the so-called "public" internet is in fact relatively secure (much more than faxes and mail). Solutions such as encryption, networks like the Health Intranet, etc, should be used where practical. But often that's not practical. We know that this is not a view shared by all! But years of experience dealing with internet issues, and the way that internet networks are constructed, indicates use for making appointments, making arrangements between hospitals and GPs, and so on, is valuable (risk can be minimised by eg: using NHI patient numbers instead of names, and so on).

decided to do something electronically, the parties need to think about how they would do it (eg: email, web-based, how to get the other party's buy-in, systems to take advantage of the new process, systems to make it more robust, particularly where that's important (sometimes it's not), and so on. Thanks to Susan Minot, Barrister for her work on the appendix.

6 PROVISION OF HEALTH RECORDS TO THIRD PARTIES

6.1 One of the big benefits (with associated risk) is the increasing ease of provision of EHRs from one health sector agency to another (eg: (a) NZHIS information to and from the DHBs; (b) DHBs providing information to GPs; (c) DHBs providing access to, say, NZHIS information, to GPs via their own networks and access links and (d) payment handling via Healthpac and other providers). As identified at the start of this paper, nothing should stand in the way of this, but there are risks that should be minimised.

6.2 What responsibility does a health provider have when it allows another to access its information? A particularly important point is that a health agency does not exonerate itself from responsibility by having its own security regime in place and simply giving information or allowing access to third parties. It can't just do a Pontius Pilate. For example, Rule 5(2) of the Health Information Privacy Code provides that when third party access is given, *"everything reasonably within the power of the health agency is done to prevent unauthorized use or unauthorized disclosure of the information."*. Even getting a recipient of the information (such as a GP) to sign something acknowledging that he or she will comply with privacy legislation is not enough. The code requires a much higher level of reassurance about the third party access and use of the information.

7 HEALTH SECTOR STANDARDS

7.1 That's a convenient point to turn to the legal implication of standards. There are several that apply. They are not legally compulsory. But they are a benchmark that may be used by judges, tribunals and others to determine whether a health agency has met required standards. This includes both the Privacy Commissioner and the Health & Disabilities Commissioner (both of whom have applicable privacy requirements in their Codes).

7.2 A useful starting point of course is *AS/NZS 17799: 2001 Code of Practice for Information Security Management*. Likewise, health sector agencies would be prudent to have regard to, and follow as appropriate, the New Zealand standards, particularly *Health Records NZS8153: 2002* and *Health Network Code of Practice SNZ HB 8169:2002*. These need to be looked at practically, with a careful eye on legal, security and privacy risk, but with major regard to the ultimate goal of better health and patient outcomes, coupled with cost and time efficiencies.

7.3 Note however that, while the *Health Records* code is relatively fluid to accommodate various circumstances, the *Health Network Code of*

Practice is relatively prescriptive in approach. For example, it requires EHRs to be communicated on a highly robust PKI model, with all participants having an internal security policy implemented, which has been independently audited. That includes everyone ranging from DHBs through to sole GPs (although of course the policy implemented for a smaller organisation such as a GP's practice is must less comprehensive and stringent than a larger organization). That simply is not going to happen in the short term and strict compliance will mean that the EHR movement would be greatly hampered.

7.4 I am not at all suggesting wholesale disregard of the Standards. Rather, the issues should be considered, confronted, moves made to change requirements or risks taken, on a calculated basis.

7.5 Note that while the *Health Records* standard is relatively fluid in approach, it is prescriptive in parts (for example, all identifiable patient data transmitted by external networks (eg: by internet email) must be encrypted (see 15.1.6).

7.6 Before leaving Standards, we should mention SSC's E-government unit. Their current authentication project seems to be focusing on situations where a lower level of authentication is required than is appropriate for health records. There doesn't seem to be focus at present on higher end security needs, other than the government to government SEE project. It's desirable though to move to public sector consistency.

8 POLICIES

8.1 The various policies (for staff, third parties, operational, disaster recovery, etc) can of course be driven by and modeled on the Standards noted above, as well as, in particular, Rule 5 of the Health Information Privacy Code. The Code is a legal requirement (and its commentary relies on the Standards). Legally, compliance with the Standards' requirements is prudent but is neither always required nor appropriate. Again, take a calculated and cautious approach when the Standards will not be met.

8.2 Circumstances vary so much that it's hard to be prescriptive. Buy-in should be achieved by careful acceptance by affected individuals, signing in handwriting not on-line, unless it's decided to take that risk.

9 CONCLUSION

9.1 EHRs offer great benefits, yet come with legal, privacy and other risks. Those risks can't be eliminated. Benefit and risk need to be balanced, and the barriers to reduce the risk shouldn't be set too high. The risk shouldn't be ignored. Rather it should be confronted.

APPENDIX:

EXAMPLES OF LEGISLATION AFFECTED BY THE ELECTRONIC TRANSACTIONS ACT

RETENTION OF HEALTH INFORMATION

Retention of health records is covered by the *Health (Retention of Health Information) Regulations 1996* which already provide for health information to be retained electronically. For this reason the ETA is unlikely to have a significant impact on the requirements on providers around retention of health information.

The Regulations require "health information" (as defined) to be retained for a specified minimum period (being 10 years in relation to the first treatment episode for an identifiable individual).

The Regulations (reg 2) define "health information" as follows:

> "health information, in relation to an identifiable individual, means—
> (a) Information about the health of that individual, including that individual's medical history:
> (b) Information about any disabilities that individual has, or has had:
> (c) Information about any services that are being provided, or have been provided, to that individual:
> (d) Information provided by that individual in connection with the donation, by that individual, of any body part, or any bodily substance, of that individual"

Regulation 9 is important, as it provides that health information may be retained in such form as the provider thinks fit, and may be retained in different forms at different times. Thus health records may already be kept electronically without the need for a paper copy.

Reg 9(2) states that where health information is kept in a form which may deteriorate before the expiry of the minimum retention period, with the result that it cannot be read or retrieved, it is sufficient compliance if an accurate summary or interpretation if the data is made and retained for the balance of the retention period.

Note that this is a somewhat *lower standard* than in section 25 of the Electronic Transactions Act which requires an electronic form of retaining records to ensure that the information is "readily accessible to as to be usable for subsequent reference".

HEALTH RELATED STATUTORY WRITING/SIGNATURE REQUIREMENTS WHICH MAY BE SATISFIED ELECTRONICALLY UNDER THE ETA

Many transactions within the health sector are not covered by the ETA because they fall outside the scope of statute (for example, transactions relating to the funding and purchasing functions of DHBs, and communications between health professionals). However there are a number of health "transactions" that do fall within the scope of the ETA because they flow from statutory writing, signature, record retention or document production requirements.

Below is a cross-section of health-related statutory and regulatory writing and signature requirements which will be subject to the ETA after it comes into force.

In each case the parties to the transaction or communication will need to determine whether there is any advantage to be gained (whether in terms of cost, accessibility or administrative efficiency) in moving to an electronic method of transacting. Advantages are most likely to be obtained where:

(a) There is a high volume of transactions/communications
(b) An electronic method (such as digital signature or certificate, or web site availability) is able to be implemented easily and without high cost to the organisation.

Cancer Registry Act 1993, section 6

Section 6 provides:

> 6 Director-General may require supply of further information
>
> (1) Where any report made under section 5 of this Act is incomplete in any respect by reason that the person making the report does not have available to that person certain information necessary to enable a complete report to be made, the Director-General may, for the purpose of obtaining that information, *by notice in writing* require any person (being a medical practitioner or the person in charge of any hospital) that the Director-General reasonably believes may have all or any of that information to provide to the Director-General such information as may be specified in the notice.

Section 5 reports require laboratories to report the presence of cancer to the Cancer Control Registry, and also following a post-mortem where a person has died of cancer.

Following the ETA, the Director-General's "notice in writing" requirement will be able to be satisfied by sending an e-mail or other electronic form of notice to the hospital being required to supply further information.

Food Act 1981, section 8B (Application for exemption from Food Hygiene Regulations)

Applications for licences and exemptions under the Food Act 1981 are administered by local authorities and public health units of DHBs.

Section 8B provides:

> 8B Applications for exemption
> (1) Subject to section 8C of this Act, any person may apply to the Director-General or the relevant territorial authority for an exemption from the provisions of the Food Hygiene Regulations 1974 in respect of any premises of the applicant, or any vehicle of the applicant, or both.
> (2) Every application for an exemption shall—
> *(a) Be made in writing; and*
> *(b) Be in the form provided or approved by the Director-General or, as the case requires, the territorial authority for that purpose; and*

(c) Be accompanied by the prescribed fee (if any).

Currently applications are required to be made in writing. Once the ETA comes into force, section 37 of the ETA will apply to this provision to allow an electronic form to be prescribed by the agency authorised to prescribe the form (in this case the D-G of Health or the TLA), and further, the agency prescribing the form will be permitted to prescribe further requirements in connection with the use of the form. This could include requirements around digital signatures, for example.

The D-G or TLA could (for example) require that if the form is submitted electronically, a digital signature of the applicant must be attached to the form.

Duty of DHBs to provide health information about individuals

Section 22D Health Act 1956

This section provides:

> (1) The Minister may at any time, by notice in writing, require any district health board to provide, in such manner as may from time to time be required, such returns or other information as is specified in the notice concerning the condition or treatment of, or the [services] provided to, any individuals in order to obtain statistics for health purposes or for the purposes of advancing health knowledge, health education, or health research.
> (2) Subject to subsection (3), it is the duty of a district health board to provide the returns or other information specified in a notice given to it under subsection (1) within such time, and in such form, as is specified in the notice.

This power to require health information from DHBs is currently exercised by the Ministry of Health under delegated authority from the Minister. Once the ETA comes into force the Ministry will (with the consent of the DHB in question) be entitled to generate and send the notice electronically under this section provided that the safeguards in Subpart 2 of the ETA are met.

Minister may by "written notice" to DHBs require them to supply specified information

Section 44 of the New Zealand Public Health and Disability Act 2000 provides that the Minister may by *written notice* to a DHB require it to supply any specified information relating to the operations of the DHB or any of its subsidiaries.

This power is likely to be exercised under delegated authority by the Ministry of Health, and once the ETA comes into force the "written notice" requirement will be able to be satisfied by electronic notice provided that the consent requirements and other safeguards under Part 3 of the ETA have been met.

Health Inquiries – requirements to produce documents

Part 5 of the *New Zealand Public Health and Disability Act 2000* provides for the Minister of Health to appoint special inquiry boards to inquire into matters concerning the funding, administration or management of health and disability services.

Under section 82 these inquiry boards have powers to investigate and summon witnesses.

Under the ETA requirements under this section for books or other documents to be produced to the inquiry, will be able to be satisfied by producing the book or document in electronic form provided that the requirements and safeguards in section 28 of the ETA have been satisfied.

DHB Boards – Procedural requirements

Under the ETA various DHB Board procedural requirements under the NZPHD Act which currently require either writing and/or signature, will be able to be satisfied by electronic means, including:

- Resignations of Board members and chairs (currently required to be in writing, Sch 3(6), (11))
- Written notices relating to quorum for board meetings (Sch 3(25))
- Delegations of board functions to committees (Sch 3(39))
- Entry into contracts and other enforceable obligations by the Board (there are writing and signature requirements) (Sch 3(42))

Similar writing/signature requirements also apply to boards of Pharmac, NZBS and RHMU under Schedule 6 of the NZPHD Act and these will also now be able to be satisfied electronically.

Mortality Review Committees

These committees are governed by Schedule 5 of the NZPHD Act. The Schedule requires various things to be in writing including:

- Notice in writing by chairperson of a committee to any person requiring that person to give information to the committee relevant to the performance of the committee's functions (Sch 5(2))
- Notice in writing by the Minister authorising disclosure of personal information for a criminal investigation or to a commission of inquiry (Sch 5(6))

Medicines Act 1981 and Medicines Regulations 1984

There are various writing and signature requirements under the Medicines Act and Regulations which when the ETA comes into force will be able to be satisfied electronically. These include:

- Applications for the Minister's consent to distribution of a "new medicine" under section 20 (notice currently required to be deposited with the Director-General of Health but under the ETA will be able to be lodged electronically)

- Applications for licences to manufacture, sell, pack or label medicines (section 17, 50 and Schedules to Medicines Regulations) which currently require writing and signature

- Issue of a licence under Part 3 of the Medicines Act by the licensing authority (section 51) – arguably no "paper" licence will be required, although note that there is a display requirement under section 54 of the MA.

- Analyst's certificate under section 71 (currently required to be "signed" but could be issued electronically with a digital signature)

- Written notice by Medical Officer of Health requiring practitioner (etc) to supply information about the prescribing or supplying of any medicines (regulation 44B Medicines Regulations)

- Medicines data sheets are currently required to be in paper form (regulations 51-54)

Note that medicines sales records (i.e. the Sale of Medicines Register) may now be kept electronically by retailers (including pharmacists) under changes to the Medicines Regulations made in 2000 (Part 11 of the Medicines Regulations refers).

Medicines prescribing requirements (including writing and signature) have been excluded from the ETA, and may now be set or varied by the Director-General of Health under regulation 43.

Health and Disability Services (Safety) Act 2001

This recent Act governs certification and quality standards for health and disability

There are various writing and signature requirements under the Act that after the ETA may be able to be satisfied electronically, including:

- Written notice of certification by the Director-General of Health to a provider of health or disability services (section 26)

- Cancellation of certification (section 30) by written notice of the D-G

- Written notice by the provider to be certified of certain information relating to certification (section 31)

- Written notice of cancellation of a private audit agency's designation (section 39)

- Written notice by the Minister of approval of standards under the Act (section 13)

Health Entitlement Cards Regulations 1993

These Regulations govern the issue of community services cards, high use health cards and pharmaceutical subsidy cards.

They contain requirements for cards to be issued with a distinctive pattern or design (see regulations 7, 18 and), but because the form for the CSC and HUHC can be determined by the Director-General of Health, it seems that section 37 of the ETA applies to enable these cards to be issued electronically. If that is the case, then a person could produce their card electronically to demonstrate entitlement for health subsidies.

The practicality of issuing cards this way is uncertain – there is a requirement for a card to bear the signature of the cardholder and this requirement may be difficult to satisfy where a card is issued electronically.

Wigley & Company is a specialist technology (including IT and telecommunications), procurement and marketing law firm founded 11 years ago. With broad experience in acting for both vendors and purchasers, Wigley & Company understands the issues on "both sides of the fence", and so assists its clients in achieving win-win outcomes.

While the firm acts extensively in the commercial sector, it also has a large public sector agency client base, and understands the unique needs of the public sector. While mostly we work for large organisations, we also act for SMEs.

With a strong combination of commercial, legal, technical and strategic smarts, Wigley & Company provides genuinely innovative and pragmatic solutions.

The firm is actively involved in professional organisations (for example, Michael is President of the Technology Law Society and Stuart van Rij its secretary).

We welcome your feedback on this article and any enquiries you might have in respect of its contents. Please note that this article is only intended to provide a summary of the material covered and does not constitute legal advice. You should seek specialist legal advice before taking any action in relation to the matters contained in this article.