Wigley & Company
BARRISTERS and SOLICITORS

DIGITAL RECORD KEEPING: LEGAL ASPECTS

Michael Wigley

ARCHIVES NEW ZEALAND
RECORD KEEPING FORUM PROGRAMME
25 MARCH 2004

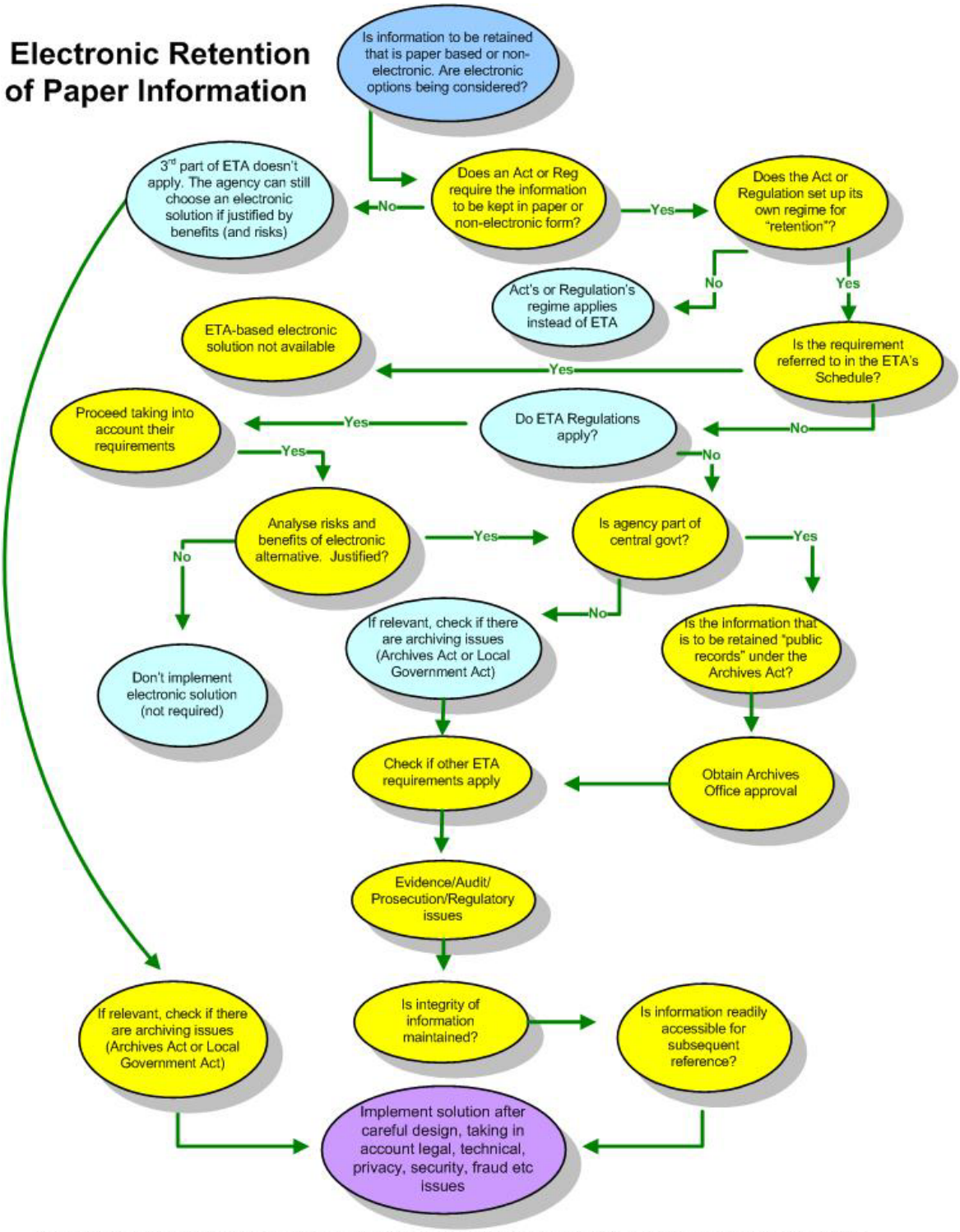
P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833
also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

MICHAEL WIGLEY started this specialist ICT, technology procurement; media law firm around 10 years ago. He is involved in a wide array of work in these sectors, ranging from large outsourcing/infrastructure computer contracts, RFPs, through to online issues, litigation/dispute issues, intellectual property, etc. He also deals with all types of procurement processes. Michael is President of the Technology Law Society and is a member of the NZ Law Society's E-Commerce Law Committee. Michael can be contacted at mwigley@wigleylaw.com

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.

© Wigley & Company 2004

Wigley & Company
BARRISTERS and SOLICITORS



Note: This diagram applies to all *legal requirements*. That includes Acts, Regulations, Orders in Council, By-laws, etc. However we have used Acts and Regulations in this flowchart for ease of reference.

Wigley & Company
BARRISTERS and SOLICITORS

INDEX

1. Introduction and overview:

1.1 The Electronic Transactions Act (ETA) is in many ways more focused on how things can be done electronically under Acts and regulations than on day-to-day commercial practices. For this reason, the ETA's impact may be much greater in practice on public sector agencies than it is on the commercial community. It has great potential to facilitate better G2P processes.

1.2 The ETA affects many processes which, by legislation, must currently be done in paper form. Now they can be done electronically. This opens the way to streamlining many of the G2P processes undertaken by public sector agencies. But generally this only has to happen where the agency so chooses (and its customers likewise choose). There's no point in doing this if there's no practical advantage, such as financial saving.

1.3 The ETA doesn't solve the problem of what systems and processes will be adequate to meet legal and practical needs. Critical from a legal

Wigley & Company
BARRISTERS and SOLICITORS

perspective is setting up the way this is done correctly. There' quite a bit of criticism of many of the systems so far, even though they are based on the so-called robust technologies, such as "PKI". A lot of careful thought needs to be put into the planning and design, not only from a legal point of view but also from a technology, privacy, security and end user buy-in point of view. Get it right and there is a great opportunity to streamline process and get stakeholder buy-in. Get it wrong, and some key drivers may not be met (such as sufficient evidence to mount prosecutions).

1.4 One thing an agency can unilaterally decide to do is to ditch its paper records and replace them with electronically stored records (which in turn can overlap with day-to-day use of those records by way of good metadata). Again the system needs to be designed carefully. For public sector agencies, there will be Archives Office issues to deal with.

1.5 In this paper I'll first scope the three key parts of the ETA, the third of which is the most important in many ways: The ETA's application to other legislation. This is the area in particular where public sector agencies' processes can be streamlined. We'll deal with a number of the legal pitfalls, which overlap also with some of the other issues such as privacy and security. We'll also deal with Archives Office issues.

1.6 Highlighted is the need to look at the specific legislation, which will vary on a case-by-case basis. Make sure the solution meets the legislative requirements, as well as operational requirements. There is no "one size fits all" solution including as to means of undertaking communications (eg: click-accept on a website, PKI, user name and PIN number, USB token etc). The ETA fits well with e-government initiatives including SSC's authentication project.

2. When does the ETA apply?

While enacted last year,[1] it won't be in force until 21 November 2003. That's because some regulations need to be passed first. So it's all about to happen. The regulations will deal with issues such as Credit Contracts and tax records.

3. 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.

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

5. What does the Act do?

The ETA boils down to three key parts.

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

Wigley & Company
BARRISTERS and SOLICITORS

5.1 Validity of electronic information.

5.2 Some default rules about place and time of transactions.

5.3 Electronic implementation of statutes and regulations.

6. **The First Point: Validity of Electronic Information.**

Electronic information is not denied legal effect solely because it is electronic.[2] There is nothing new in this. The Courts are usually great at responding to new technology developments. Generally they will enforce something that is electronic just as much as if it is paper based.

7. **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 rather than whether in principle it's appropriate. 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 all of that role to administrative staff. No amount of legal mumbo-jumbo is going to stop that. Say if there is a fraud (where ACC or the Police need to prove the case against the doctor, beyond reasonable doubt (a very high level of 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.

8. In theory the electronic evidence based on the digital certificate, using 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" by digital certificate, did in fact "sign".

9. A much lower level of proof than the criminal level applies to many other types of legal claims and disputes (including normal commercial disputes and privacy enquiries by the Privacy 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 ACC 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.

10. How often do organisations consider those types of issues? Prosecutions and other court and tribunal issues are not mainstream considerations for organizations. But they are considerations in many situations nonetheless. Many electronic processes will meet mainstream legal and practical obligations, yet fall over when it comes to prosecution. The need potentially to prosecute comes up in many public sector situations, ranging from the serious (eg: welfare fraud) to the "day-to-day" (eg: notifying scaffolding details to a local body)

11. **The electronic "signature" is not everything:**

[2] Section 8, Electronic Transactions Act

Wigley & Company
BARRISTERS and SOLICITORS

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. Money being paid into someone's account and then drawn out is pretty compelling!

12. But that doesn't get around the point that this is a difficult area and the best way forward needs to be considered and the system designed with these types of issues in mind. 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.

13. 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 Bank employee click accepts an online policy. The Bank might struggle later to prove she personally did this, so that she's bound by the policy terms. What happens when she brings a personal grievance because she is dismissed for looking at porn on-line in breach of the online policy?

14. 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 in such important areas is too risky with current technology. It's 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.

15. For a good example of potential problems, see 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. This article highlights how critical it is to design the system right in the first place (I'm not saying the IRD system doesn't work! Just that careful design of system is needed).

16. Sometimes user buy-in to policies and terms doesn't matter so much. So online click accept is OK from a risk point of view. Many G2P communications fall into this camp.

Wigley & Company
BARRISTERS and SOLICITORS

17. 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 organisation, even with important policy and contract requirements, may decide to do things on-line. This should be a calculated risk (often it's not).

18. 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.

19. **Electronic solutions are not perfect**:

    Note that for situations requiring highly robust solutions (eg: to support prosecutions) PKI based digital certificates may still be too risky. Even the most stringent methods of protecting electronic records and transactions 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, 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.

20. But the big legal problem lies around the 4th attribute: *authentication* (ie: confirmation that the person sending or receiving the message is who he says he is). A big weakness for PKI 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 organisations operate in exposed security environments.

21. **What's Important?**

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

22. 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

Wigley & Company
BARRISTERS and SOLICITORS

privacy obligations. But, often, far more important is the ultimate goal of improving services overall. Often, nothing should stand in the way of that. The idea is to minimise the risk overall, in practical terms. It all depends on the particular circumstances. It's important to consider specific issues in each case.

23. **Compare with what's there at present.**

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 electronic records. For example, one of the great things about 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 (often, 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.

24. **PKI.**

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 (see http://www.anu.edu.au/people/Roger.Clarke/). 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.

25. **PINs instead of PKI.**

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.

26. 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 PKI process. For a scathing attack see Roger Clarke's submissions to the current Joint Parliamentary Audit and Compliance Select Committee hearing (http://www.aph.gov.au/house/committee/jpaa/electronic_info/submissions/sub51.pdf).

27. I'm not saying that a PIN approach is preferable, nor that PKI is unsuitable. Rather, there are options to consider, depending of the application. Certainly, a "one size fits all" is not a good approach.

Wigley & Company
BARRISTERS and SOLICITORS

28. 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

29. **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 organisation is doing, but generally that would not be the case.

30. **The Third Part: 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]

31. Acts or regulations do not directly cover many things that happen in the business and public sectors. 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 (and so is usually unaffected by the Act as a whole). The same applies to many other transactions, records etc. Their creation and use is often not driven directly by acts or regulations. So the ETA makes little or no difference.

32. **Other Acts and Regulations:**

Other Acts and regulations can have effect anyway, overriding or supplementing the ETA. In the health sector, 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 being whether the electronic health records can be accessible over the required 10-year period in view of changing technology etc (Regulation 6 and 9).

33. This highlights the need to address each specific situation.

34. **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 in some circumstances. Sometimes a PKI based digital certificate may not be enough because of its uncertainties as noted above. There

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

Wigley & Company
BARRISTERS and SOLICITORS

is a default provision to define the perfect signature but, arguably, even PKI doesn't meet its needs.

35. Covered is means of giving access and providing 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.

36. **Tax Records.**

Records which are important to many organisations are tax records. They often have to be retained for 7 years. Under the new regulations, it's likely that 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.

37. 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 for tax purposes. 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.

38. **Exclusions under the ETA.**

A number of Acts and Regulations are excluded from the ETA[5] but these are quite limited except in particular sectors (eg: health).

39. **What Records are Covered by the ETA?**

There are thousands of statutes and regulations where change is possible (or required) due to the ETA. By way of example, we've set out some illustrations in the appendix below from the health sector. It's important (especially for public sector agencies) to check applicable statutes and regulations, and decide what to do, taking into account what's needed for legislation, and to achieve desired outcomes and cost benefits. If it's 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), software suitable for storing information and so on).

40. **Retaining records and the ETA.**

Under the third part of the ETA, both parties to an affected communication must agree before there can be electronic compliance with statutes and regulations.

[5] See the Schedule to the Electronic Transactions Act

Wigley & Company
BARRISTERS and SOLICITORS

However, retaining records is not necessarily transactional in this way. Therefore organisations have decisions to make.

41. Importantly:

    41.1 They're not forced to record electronically (so this should be done only if there are advantages in doing so).

    41.2 The ETA in this part applies only to legislative record keeping requirements. Many records don't have to be retained for legislative reasons, so the ETA doesn't apply. See below however about the Archives Act.

    41.3 If another Act or regulation governs record keeping, that applies instead (see for example the Health (Retention of Health Information) Regulations 1996) as noted above).

    41.4 Organisations should carefully decide what to do (and whether to implement) before launching their on-line projects (taking into account legislative, commercial, practical, legal, security and privacy issues, etc).

42. For electronic record retention under the ETA the starting point is that information can be recorded electronically if "*... the information is readily accessible so as to be usable for subsequent reference ...*".[6]

43. This raises the obvious question about whether the information can be accessed later (eg: if there are problems caused by obsolete software, etc). The suitable approach will depend on the circumstances, the length of time the information should be retained, whether other software could later access the information if the current software becomes unusable, etc. We expand on this below in relation to the Archives Office requirements.

44. **Format and Layout.**

    Generally, the information doesn't have to be kept in the same format and layout as the legislation requires for paper-based record keeping (s.21).

45. **Integrity of the Information.**

    If the organisation retains the information electronically, when the relevant legislation otherwise requires paper based recording or the like, this can happen under section 25 if:

    45.1 "the electronic form provides a reliable means assuring the **maintenance of the integrity of the information**; and

    45.2 the information is "readily accessible so as to be useable for subsequent reference"; and

[6] s.19. Note the special requirements referred to above for tax records.

Wigley & Company
BARRISTERS and SOLICITORS

45.3 if it's a "public record" under the Archives Act, the Archives Office has approved retention electronically.

46. I've put in bold the reference to maintenance of the integrity of the record as section 17 deals with this requirement. To meet it, the information needs to be complete and unaltered, except for immaterial changes arising during normal storage (that would be indexing data and so on). Again, depending on needs and circumstances, this requires software and systems that reassure that the record is unaltered (or, depending, unalterable).

47. There's the same type of rules for other electronic processes (such as for retention, where required, of details of electronic communications.[7]

48. **Archives Office Requirements:**

The Archives Act applies to retention of "public records" in central government. These are very widely defined and include electronic records. There are comparable requirements for local government under the Local Government Act. Broadly, if a central government agency has a "public record" which is in paper form, it could not be converted into electronic form (eg: scanned) without blessing from the Archives Office. Similar rules apply for local government. This was the position before the ETA.

49. The ground rules in this area are about to change, with new Public Records legislation being drafted at present. The ETA makes clear expressly in respect of central government, and in any event often in respect of local government as well, that the public sector agency can't simply convert paper records which are "public records" into electronic form. They need to get approval from the Chief Archivist.

50. Details of Archives' processes and the proposed new legislation are set out at www.archives.govt.nz/continuum.

51. Surprisingly, only a handful of agencies have sought permission from the Archives Office to transfer paper records into electronic form. Thus far, Archives are handling these requests on a one-off basis. But sooner or later no doubt a standard practice will develop, as envisaged by the ETA.

52. Archives (and anyone else concerned about document retention) take a holistic approach. They don't just focus narrowly on issues such as whether PDF software will be supported in 5 years. They look at a number of issues including:

- the medium in which the information will be stored (there is some evidence for example that information on CD ROMs degrades over a relatively short time frame);

[7] s.27.

Wigley & Company
BARRISTERS and SOLICITORS

- the prospect that the document management software (whether scanned, TIF, proprietary documents management system or whatever) may no longer be useable in future; and

- the document retention policy of the agency in general.

53. For example, an important issue may be to ensure there is a system in place which has the information transferred to another medium or system when the current medium or system becomes outdated or obsolete. In other words, archivists will tend to take an overall management approach in this area and not just focus on the immediately available technology.

54. Apparently, local government has been strongest in pushing down the electronic storage path. Of course these are the benefits to be gained not only in terms of storage of information but also in terms of ready access to information, utilising metadata.

Summary

The ETA, within its scope, provides plenty of opportunity to streamline processes. But application in each instance needs to be carefully considered, taking into account not just the ETA but also additional legal and other issues. This requires careful and holistic legal review. The Act is generally flexible to meet needs. Where electronic material could be used for prosecutions, particular care is needed.

Wigley & Company
BARRISTERS and SOLICITORS

APPENDIX: EXAMPLES OF HEALTH RELATED 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".

Wigley & Company
BARRISTERS and SOLICITORS

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:

Wigley & Company
BARRISTERS and SOLICITORS

> 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 Director-General of Health or the Local Authority), 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 Director-General or the Local Authority 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

Wigley & Company
BARRISTERS and SOLICITORS

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.

Wigley & Company
BARRISTERS and SOLICITORS

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)

Wigley & Company
BARRISTERS and SOLICITORS

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.