Wigley & Company

BARRISTERS *and* SOLICITORS

ELECTRONIC HEALTH RECORDS: 2006 LEGAL UPDATE

May 2006

P O Box 10842 • Level 7 • 107 Customhouse Quay • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833

also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

Wigley & Company

BARRISTERS and SOLICITORS

In May, Michael Wigley addressed the Conferenz Medical-Legal conference and the Brightstar Electronic Health Records Conference.

INDEX

1. Introduction

1.1. This paper summarises more recent developments. There are a number of papers on our website that set out more detail that is not covered here, including:

1.1.1. *Electronic Health Records – Legal Issues*[1]

1.1.2. *Privacy implications for information technology*[2].

1.1.3. *IT Security and the Law*[3]

2. Overview

2.1. From any perspective (including legal) EHRs cannot be perfect fail-safe solutions. There are many factors to take into account. Solutions must take account of issues such as:

2.1.1. Improved health outcomes;

---

[1] www.wigleylaw.com/Articles/LatestArticles/ElectronicHealthRecords/

[2] www.wigleylaw.com/Articles/LatestArticles/privacy-implications-for-information-technology/

[3] www.wigleylaw.com/Articles/LatestArticles/legal-developments-in-it-security-/

2.1.2. Overall health cost savings;

2.1.3. Security;

2.1.4. Privacy;

2.1.5. Robust service levels, availability and reliability of the service;

2.1.6. Ability to access quickly in emergency situations (break glass);

2.1.7. Reputational risk;

2.1.8. Evidential proof where that is required (eg: "*Beyond reasonable doubt*"/"*balance of probabilities*").

2.1.9. Controlled access (with a "*break glass*" override) via appropriate authentication vehicle;

2.1.10. Benchmarking against the imperfect hardcopy world;

2.1.11. Project risk (eg: decentralised v. centralised approach; "*big bang*" v. incremental approach).

2.2. I'm not sure that all these factors (and others besides) always get the attention they deserve and require. None of these drivers can be met 100% and indeed 100% solutions to each of these drivers would not be desirable (for example 100% privacy protection would make the system unworkable).

2.3. A holistic approach is called for. Silo approaches (eg: a project taken over by a zealot interested in a particular issue or someone undertaking the project without regard to all relevant issues) are dangerous. For example, the privacy impact assessment (PIA) methodology is excellent but, in the wrong hands, can lead to a stand-alone approach which focuses unduly on privacy at the expense of other key drivers. The PIA should be undertaken in the context of the overall requirements.

2.4. The law generally supports and allows solutions that are not "*100%*". For example, HIPC Rule 5(1) requires health agencies to hold health information in a way that ensures it is protected "*by such security safeguards as it is reasonable in the circumstances to take ...*". While of course sensitive and personal health information calls for heightened security treatment (and anyway excessive security breaches will lead to project failure), that does not require 100% security protection. 100% security and privacy solutions would be unworkable and in turn lead to greatly reduced health outcomes. The latter is a key driver and thus the system should be robustly but not 100% reliable with, subject to appropriate access controls, a "*break glass*" auditable solution in emergency situations.

2.5. While it is said that health information is the public's second highest priority privacy issue, compared with other privacy issues, what would the answer be when the question is stacked up against reduced health outcomes due to heightened privacy compliance?

2.6. Implicit in EHR regimes is the exchange of information between agencies. HIPC Rule 5(1)(b) confirms that, where it is necessary for information to be given to another "... *everything reasonably within the power of the health agency is done to prevent unauthorised disclosure of the information* …". This means that an agency receiving health information cannot simply pass on the information to another agency. It has to have sufficient reassurance about prevention of unauthorised use and disclosure. There are various solutions including agreements between agencies, standards compliance, and so on.

2.7. In relation to authentication, the approach can reflect the relatively closed group of personnel within the sector, ranging from clerical to specialists. As our other papers identify, there can be problems around authentication for a number of reasons. But some compromise (in terms of quality of authentication) is appropriate within this community. A different approach may well be necessary in relation to patients' electronic access to information remotely. In relation to informed consent generally from patients, some at least are taking an "*opt out*" type of approach but it seems prudent with current technology for a clear-cut "*opt in*" approach where health information is to be communicated electronically directly to and from the patient. Subject to that opt-in solution, it may be appropriate to facilitate unencrypted email communications (depending perhaps on the subject matter of the email). Authentication of patient access to an intranet would need to be carefully handled.

2.8. The Privacy Commissioner's commentary on the Health Information Privacy Code indicates that the required steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of the intended use of the information etc, can be met by an oral explanation, notice on display in the health agency's premises, brochures and an explanatory note on standard forms used for collecting health information. The requirements may vary according to culture, language, physical and mental disability barriers etc. How detailed the explanation should be will also depend on the circumstances. Arguably this is a surprisingly low threshold for HIPC Rule 3 compliance but then it does have the blessing of the Privacy Commissioner and it does make much more workable obtaining informed consent.

2.9. In an ideal world there would be a clear-cut "*opt in*" approach by which the patient generally signs a document that refers in clear fashion to the intended use of the information etc. In the absence of that, there is always a risk that either the health professional will not in fact give an appropriate explanation or, just as likely, that the patient will later say that the explanation was not given when in fact it was. These are the types of issues that need to be balanced and assessed when schemes are put in place. This is not at all an easy area and it is made more problematic because each case will depend on its own circumstances. But at least the Commissioner indicates a more relaxed approach is acceptable.

2.10. There is a Privacy Act review currently underway and this provides an opportunity for further input if it is considered that there should be changes to the Privacy Act.

3. Buy-in from Health Professionals

3.1. It's surprising how slowly there is buy-in from some health professionals to the need and desirability for EHR. I wonder whether the situation will develop such that failure of a clinician to utilise EHR (including providing information and using it) will be negligent or in breach of disciplinary rules. Sadly, perhaps it will be adverse outcomes for professionals at inquests and disciplinary hearings that may drive the professionals' acceptance of the system rather than buy-in for the right reasons.

4. Electronic Transactions Act

4.1. There are a number of Acts and Regulations which are excluded from the application of the Electronics Transactions Act (ETA), including health-related legislation set out in our earlier electronic health records paper. The Ministry of Economic Development (MED) has undertaken, as is it required to do under the Act, a review of which legislation and regulations should remain excluded from the ETA. Regulation 41 of the Medicines Regulations 1984 sets out the required form of a prescription. It is excluded from the ETA and therefore must be a physical document and signed by the prescriber in handwriting. Yet of course there are great cost savings and efficiencies (and reduced risk of error) by way of electronic prescribing. This is a driver in the New Zealand health sector, as is confirmed by the "*Health Information Strategy for New Zealand 2005*" produced by the Health Information Strategic Steering Committee.

4.2. However the Regulations have been amended by adding (at Regulation 43) that the Director-General of Health may "*in special circumstances and at his or her discretion … authorise a form of prescription that does not comply with all or any of the requirements in Regulation 41, but that is subject to any other requirements that he or she thinks fit …*".

4.3. The February 2006 MED review of the ETA includes the following statement: "*This means that the Electronic Transactions Act does not apply, but the Director-General of Health may authorise electronic prescription systems, including pilot schemes. This solution facilitates implementation of a co-ordinated, and technologically reliable and consistent electronic prescriptions regime*".

4.4. Over time, electronic prescriptions can be expected to be the norm rather than the exception yet Regulation 43 seems directed at exceptions rather than the normal situation. We consider that electronic prescribing should be undertaken as specified by the Director-General (this will enable development of a standard and inter-

operable approach) but that the words "*in special circumstances*" in Regulation 43 should be removed (or there should be some other solution).

Wigley & Company is a specialist law firm founded 14 years ago. Our focus includes IT, telecommunications, regulatory and competition law, procurement, and media/marketing. 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).