

The implications of data privacy legislation for the development of hospital information systems

Reeva Lederman

Abstract

This research provides an analysis of the implementation of medical data privacy law in Australia, with emphasis on the Victorian Health Records Act 2001 (HRA). We examine the ability of health organisations to respond to the requirements of this legislation, and similar health privacy legislation elsewhere, and illustrate that this ability is affected by the quality of their patient data and the structure and security of their databases. This article suggests that compliance with the legislative provisions creates implications for information systems development and design, which large public and private hospitals have so far failed to consider or act upon.

Keywords: *Health Records Act Vic, 2001; data privacy; health information management; information systems design; data quality.*

Introduction

Over the last two decades, there has been increased concern and interest worldwide in the area of data privacy. In October 1995, the European Union (EU) enacted the Data Privacy Directive following many years of discussion and debate (EC/95 1995). Article 25 of the directive prevents members of the European Union transferring data to jurisdictions where privacy is not adequately protected as defined by the EU's Information Privacy Principles (IPPs; see Appendix). These requirements have imposed obligations worldwide in both the business and health sectors, with privacy legislation being enacted not only in Europe, but also in the US, Canada and Britain, as well as in Australia.

In Australia, the confidentiality of health information has historically been governed by a plethora of different standards administered by various Federal and State bodies, as well as case law (particularly, *Breen v. Williams* 186 CLR 71). The *Commonwealth Privacy Act 1988* introduced the concept of Information Privacy Principles (IPPs), and public health providers, like other public authorities, have been bound by Freedom of Information principles since 1982. However, this legislation is not specific to the health sector. While a Victorian Information Privacy Act already existed prior to the enactment of the HRA, this Act only applied to the public sector and funded agencies, while health service providers cover an array of entities across both the public and private sector.

The disparity and fragmentation of these various laws was part of the impetus for the creation of some uniform standards in Victoria resulting in the Victorian Health Records Act, which came into effect on 1 July 2002, with compliance required for most health providing entities. The HRA is based on the principle of maintaining the privacy, confidentiality and security of medical data by promoting the fair and responsible handling of health information. These objectives of privacy, confidentiality and security are also central to British health-privacy legislation and are defined in a National Health Service report (National Health Service, 2001) based on the same core EU principles as follows:

- *Privacy*: the right of an individual to retain personal information to themselves (which may include the right to suppress information held by

others). This relates directly to the parts of the HRA concerned with how information is used.

- *Confidentiality*: the duty to keep secret privileged information received or concerning others, to prevent loss, damage or embarrassment to those concerned. This relates directly to those parts of the HRA concerning disclosure of information.
- *Security*: the need to keep information accurate and reliable and only available to those properly authorised to access it. This includes those parts of the HRA preventing loss, corruption, or access by those not properly authorised — it also includes ensuring that the data is available and accessible to those who should have it.

The HRA seeks to strike a balance between assuring an individual's health information is protected while allowing the flow of necessary health information. Stevens (2003), in a report on similar US legislation (the Medical Privacy Rule), raised the difficulties of achieving these objectives. She criticised the US legislation, on the grounds of its complexity, the likely difficulties in compliance, likely cost of compliance and the lack of technical assistance for compliance. Stevens claims that health privacy legislation worldwide has created significant concerns among health providers.

Twight (2002) has suggested that worldwide privacy legislation has been complex and difficult to implement. We see in fact that these difficulties have been recognised in Victoria for decades. Varghese (1982), commenting on the Freedom of Information Act (FOI), suggested that the state of data holdings in the large public institutions governed by the FOI would require much attention from records managers and it would be difficult to "develop, maintain and update information systems" to the extent required for compliance. The question in this research is whether the current state of information systems in large hospitals today (where there is a requirement to handle an even greater volume of both electronic and paper records than there was when the FOI was introduced) makes them any better prepared to overcome these difficulties.

What is striking about the HRA is the extent to which it requires the health-providing organisation to have control over its patient database in order to ensure appropriate levels of access and distribution of data. For example, the legislation demands that in

most cases individuals should be able to have access to their full medical record while use and disclosure of data to other individuals is restricted (IPP 2 & 6). Individuals should also have access to protected information (IPP 2) and a right to request privacy protection even where the HRA may permit disclosure (IPP 6). These provisions and many similar ones all require the relevant health provider to exercise complete control over the data it administers and how that data is stored and distributed, and the reliability and quality of the data.

In all large organisations there are difficulties in ensuring the quality of organisational data (Redman 2001; Wang 1998) where, at a minimum, good quality data is seen to be accurate, complete and verifiable (Stair 1992). We maintain that it will be difficult for a large health provider, such as a major hospital, to achieve the level of data quality required without high levels of investment in information infrastructures. Such investment has traditionally been lacking in the hospital sector (England 2001; Starr 1997).

Hospitals have generally introduced information systems in an ad-hoc manner, initially installing basic patient admission and discharge systems and then adding stand-alone systems to support other patient functions such as imaging. This approach results in a highly fragmented patient record with a complete view often being unavailable in large hospitals. Such fragmentation is well documented in the health system (Bloom 2003; Junnakar 2003), where "health-care organisations are notorious for huge legacy infrastructures that don't interface" (Schulten 2001). This results in significantly decreased ability for patients to have access to their full patient record, despite this being a primary right under the new legislation. While the press report the need for large sums to be invested in order to implement similar legislation overseas (Perry 2001), these estimates do not cover the cost of full database integration and security controls. There is also no indication that these measures have been factored into the cost of implementation in Victoria.

In sponsoring the Bill, the Member for Gould stated that "the government recognises, and is responding to, community concerns about the threat of privacy posed by the exponentially increasing capacity of modern technology. While new technology brings many benefits for individuals and the community as a whole, the potential exists for technology to be misused, and for people to suffer discrimination or other kinds of harm as a result. Nowhere is this more evident than in the case of health information. . ." (Victorian Government, 2001). We see in this research, however, that while there are threats to individual privacy inherent in the use of information technologies, the use of appropriate technology, suitably managed, can in fact enhance health care users' opportunities for privacy protection.

We argue in this article that to implement the objectives of the *Health Records Act 2001* it will be difficult for health providers to ensure that the data they hold is structured and managed in such a way as to be of sufficiently high quality to provide the full access to and maintenance of accurate records that is required to satisfy the legislative provisions. This will also be the case for hospitals in other jurisdictions that have

privacy legislation based on the same EU privacy provisions.

Research Questions

To explore this issue we consider the following research questions in this article:

- Do the methods of data management in large hospitals allow these hospitals to satisfy the key legislative requirements of the *Health Records Act 2001* of access to the patient record, appropriate use and disclosure of the record, and opportunities for correction?
- What are the implications of the findings in this article for information systems development in hospitals?

Methodology

This research was conducted in early 2004 and involved an initial preliminary study of relevant legislation and literature, including an extensive review of the HRA. Next, the components of the three issues of privacy, security and confidentiality, as expressed in the Information Privacy Principles in the legislation, were considered, as well as their relation to problems of collection (IPP 1), use (IPP 2), disclosure (IPP 2) and access and correction (IPP 6). A set of interview questions, which focused on the approach hospitals were using to ensure compliance with these aspects of the legislation, was developed.

The data collection stage of the study involved eight in-depth interviews in five public and three private hospitals with relevant hospital employees, four of whom were health information officers managing a privacy portfolio within the hospital and four of whom were designated privacy and freedom of information officers. All of the interviewees had a job title and description of Health Information Manager or Manager of Health Information Services and were the most senior people in the hospital in charge of ensuring the privacy of information.

The hospitals were selected based on geographic location to give a reasonable spread across the Melbourne suburbs, and thus to capture a varied hospital population and some variance in hospital funding. Additionally, the private hospitals were also selected based on size, with larger private hospitals being chosen. The number of admissions to the public hospitals sampled ranged from approximately 36000 to 60000 inpatients per year, and the private hospitals' intake ranged from approximately 12000 to 32000 inpatients per year. All of the hospitals provided allied health services, including physiotherapy, occupational therapy, social work, nutrition and speech pathology. Records showed an average of nearly two hours per day being spent by inpatients using allied health services in the public hospitals surveyed. While the private hospitals surveyed do not collate allied health hours as they are billed to private insurers, the private hospitals also reported extensive use of these services. Consequently, all eight hospitals served patients in a manner which encouraged the development of a complex, multi-sourced, individual patient file.

The interviews all took approximately one hour and were held at the interviewee's workplace and then transcribed and analysed using qualitative data techniques (Miles & Huberman 1994).

Results

Issues of primary significance

The analysis of the data revealed a number of issues of significance that would most impede the hospitals' ability to fulfil the requirements of the *Health Records Act 2001*.

Managing fragmented databases

At all of the hospitals surveyed, non-integrated databases were a significant problem, providing a major impediment to both collection of and access to data. At one hospital, the information officer acknowledged the existence of a non-integrated cardiology database; at others, psychiatry was stand-alone; at another, psychology and assault clinic information was collected separate from the central file; while at yet another, transplant services were separate. At almost all centres, allied health services such as physiotherapy were not integrated with the main patient record. One information officer stated:

Any stand-alone record, aside from the main record, from a health information perspective and from this whole privacy perspective, is an issue. When we do have privacy requests from a client who wants to access their file, or a third party or whatever, they potentially don't know about this other information that isn't being accessed.

At one hospital where patients had an opportunity to use the facilities of a number of health services away from the main campus, the information officer acknowledged that patients requesting their record were only given the notes held by the main hospital because other notes were too difficult to access. This was despite "a documented policy that is fairly recent and prohibits the use of decentralised record keeping across the organisation".

At one hospital, the central records staff identified significant problems with the maintenance of full test results that appeared to also stem from the existence of a non-integrated record, and an interviewee reported:

Pathology reports are sent to both the doctor involved and the hospital, with doctors often maintaining their own databases of patient results. In cases where there is more than one doctor involved in the care, the doctor may take the hospital's copy of a test result. Sometimes we might find they're incomplete because we haven't known that the (doctor) ordered ten tests. Say we've got five reports and we think that's complete, but there could be another five outstanding. And other doctors have picked up these reports (and not returned them to the record).

None of the hospitals officers surveyed could guarantee that if a patient made a request under the HRA for access to their record the record produced for the individual patient would be a full data set extracted from all possible repositories. This was a particular problem in private hospitals, where doctors operated

consultancies independent of the central hospital organisation.

Controlling paper-based records

A second, related significant problem was the occurrence of lost records, or lost components of records, often as a result of records being maintained in paper-based form and not recorded on any of the hospitals' databases. This exposed the record to the possibility of all forms of privacy violation; for example, that it could be improperly used, accidentally disclosed to unauthorised parties, and rendered impossible for the patient to access and correct, as the following comment indicates:

It is very difficult to maintain a complete paper-based record ...where services are community based because physically the services are located out in the community... They do maintain separate notes in the community centres.

In addition, there were difficulties expressed with regard to maintaining security over paper-based records. Access to paper-based records cannot be controlled with a password as with an electronic record, nor can audit controls be reliably implemented to check who has recently accessed the record. An interviewee reported that paper-based records are sometimes misplaced:

Our entire records do on occasion go missing. And the first we know about it is when the patient represents requesting their record or rebooking and we try and find the record and it isn't where we think it is.

Previous research (Lederman 2002) suggests that lost records are commonplace across the medical world and are a significant obstacle to the ability of organisations to maintain security over records and to give patients full access to their record without missing components.

All of the hospitals surveyed in fact had a combination of both paper-based and electronic clinical records. This especially affected the implementation of aspects of the legislation relating to completeness, access and correction. Discrepancies between the information maintained in an electronic record and a hardcopy record often arose. For example, there were often delays in printing information from the electronic system and filing this information into the hardcopy record. In addition, not all the notes maintained electronically were placed in the paper record and there were not clear procedures in all hospitals to ensure this took place.

Implementing system security

Some of the information officers interviewed felt that a safely stored paper record that needed to be signed in and out of a central file location was in fact more secure than an electronic record in some regards. According to one officer: "Hospitals that have gone onto a fully electronic record don't have that locational [security]. You know, the record is everywhere."

Hospitals all reported problems found regularly by British researchers in similar environments of leaky and unreliable data security and transfer protocols (National Health Service, 2001). In many of the hospi-

tals surveyed, technical constraints restricted the ability to limit access to certain individuals. These constraints included the following, all exposing the patient record to improper use and disclosure:

- *Lack of timed log-offs.* In some settings, staff had different layers of access but would leave computers logged on and walk away from them without any automatic time-out being implemented. There were incidents in which not only junior staff but also patients accessed files where computers were left unattended.
- *Lack of audit trails.* At one hospital, staff at different levels shared generic log-ons, so it was impossible to implement an audit trail to see if individual staff examining records required access for genuine reasons. Even where staff had individual log-ons to machines, audit trails were not always implemented on particular applications containing patient files, neither was audit reporting implemented. One hospital chose to circumvent its audit process by restricting activation of audit trails, as running the program potentially slowed down the system. Another had no auditing facility at all: "We don't know at a ward level who is accessing what".
- *Lack of restrictions on removing files from the hospital.* Patient files were able to be copied and taken home on disk, with no assurance that changes made would be incorporated into a central repository. This could lead to a possibility of different, conflicting records being held for the same patient, as well as exposing the whole file to the risk of inappropriate disclosure or loss once it left the premises.
- *Access to irrelevant information.* Under use and disclosure provisions, hospitals are permitted only to maintain information that is relevant for their activities. However, a number of hospitals that shared facilities with pathology providers or allied health providers had full access to records of patients who were not actually the patients of the hospital.

Discussion

Implications for the development of hospital information systems

Recent press reports suggest that "health workers are usually acutely aware of the need to maintain patient confidentiality" (Place 2003), but the results of this research clearly indicate that the goodwill of staff is not sufficient for genuine compliance with the HRA, or any similar legislation based on the EU Information Privacy Principles.

The provisions of the Health Records Act recognise that "disclosure of personally identifiable health-care information can profoundly affect peoples lives" (Stevens 2003) and, therefore, aim to give users of the health system control over the data that is held about them. However, this research suggests that many large health organisations are not in fact able to give patients this control when the organisations themselves are maintaining fragmented and incomplete patient databases. While hospitals have stated policies

which acknowledge the desirability of centralised and integrated record keeping, none of those surveyed had a fully integrated record set or were able to readily access a full and complete medical record for any individual patient with absolute confidence in its accuracy or completeness. This problem was exacerbated in hospitals with multiple campuses, in private hospitals where doctors conducted independent consultancies, and those hospitals providing additional allied health services such as physiotherapy and pathology. In many cases, these separate units maintained their own patient records with no regular integration with a centralised database. Until these organisations not only implement stricter data collection policies, but also integrate their functional units sufficiently for a complete and unified patient view to become possible, compliance with the HRA is not feasible.

The results of an unpublished privacy questionnaire at one private hospital indicated high levels of satisfaction with the form requirements of privacy implementation. However, the common understanding of privacy by patients (or even hospital staff) can be quite different from the actual legislative requirements. Patients were asked four questions: Did you receive privacy information prior to admission? (70% said Yes); Was the content of the privacy brochure easy to read? (78% said Yes); Did you feel informed on your privacy rights? (74% said Yes); Did you feel the collection of your information was done in a fair and non intrusive way? (90% said Yes). This high level of satisfaction, however, obscures the fact that while it is important to have the fulfilment of these measures affirmed, such measures do not go to the core of the legislation that requires a patient be able to access a full and complete medical record to ensure that this record is being used appropriately and subject to verification and correction.

The implementation of security features in tandem with a fully integrated database is essential for compliance. However, in some of the hospitals surveyed, even the minimal standards evident in organisations that valued their customer data were not implemented. British researchers (National Health Service Report, 2001) have identified a long list of security issues that systems developers in hospitals need to consider, including issues of traceability, de-identification of data, security controls on links between data sets, and transfer protocols. At none of the sites surveyed had IS departments fully considered and revised security controls in the light of privacy obligations. At some survey sites, technical measures for implementing security were not available; at others, staff overrode security measures. Canadian researchers have acknowledged the difficulty in finding systems developers who knew enough about the security issues surrounding data protection principles to make systems privacy compliant (Flaherty 2000), but this is a challenge that systems developers must be encouraged to meet by hospital management.

While many hospitals in Australia have been exploring the possibilities of a fully electronic patient record in recent years (Davie 2002), it is clear from this research that such developments need to be made with full regard for the security and database integration

required to achieve the level of data quality needed to implement data privacy legislation in full.

Conclusions

While the HRA may go some way in advancing information privacy in the health care sector, the interviews detailed suggest that fundamental changes in information systems design and implementation may need to be effected before large health organisations can be genuinely compliant. While interviewees suggested that tens of thousands of dollars have been invested in privacy committees in hospitals, patient information brochures and associated measures for the introduction of the Act, little serious thought seems to have been given to the investment required to restructure hospital information systems that must go hand in hand with the introduction of this new law, even though the research was completed nearly 18 months after its introduction. However, only if hospitals understand the need to make this investment can they hope to exercise the control over patient data that the genuine provision of patient data privacy necessitates.

In an environment in which calls for hospital amalgamations and greater economies of scale are increasing, hospitals need to be asking how they will manage to integrate the massive amounts of data ensuing from these multiple sources, and what support regulating authorities will provide to help them do so.

References

- Bloom FE (2003). Science as a way of life: perplexities of a physician-scientist. *Science* 300(5626): 1680-1685.
- Davie K (2002). Next to go on-line: your medical record. *Australian Financial Review*, 10 April 2002.
- EC/95 (1995). Directive of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 20 Feb.
- England I (2001). *The status of health IT expenditure: a qualitative study of senior executives in regard to IT investment*. Proceedings of the Australian Health Informatics Conference 2001. Canberra, 29-31 July 2001.
- Flaherty D (2000). *Privacy impact assessments: an essential tool for data protection*. 22nd Annual Meeting of Privacy and Data Protection Officials. Venice, September 2000.
- Junnakar S (2003). Law prescribes overhaul of aging system. CNET News.com June 16, 2003.
- Lederman R (2002). How poor information systems increase hospital queues. *Health Informatics Journal* 8: 147-152.
- Miles MB and Huberman AM (1994). *Qualitative data analysis: an expanded source book*. 2nd edition. Thousand Oaks, Sage.
- National Health Service (2001). Lifehouse Project data protection work team. *Report on data usage, consent, ethical approvals and research controls*. December 2001.
- Perry J (2001). Medical "Privacy" rule tab \$18 billion, value \$0. NewsMax.com 18 April 2001.
- Place A (2003). Keeping patients medical records safe from prying eyes. *The Age* (Melbourne) 12 April: 2003, p: 34.
- Redman T (2001). *Data quality: the field guide*. New Jersey: Digital Press.
- Schulten C (2001). *Integration architectures in healthcare and how to extend access to mobile healthcare workers*. Proceedings of the Australian Health Informatics Conference 2001. Canberra, 29-31 July 2001.
- Stair R (1992). *Principles of information systems*. Boston Mass: Boyd and Fraser.
- Starr P (1997). Smart technology, stunted policy: developing health information networks. *Health Affairs* 16(3): 95-105.
- Stevens G (2003). *A brief summary of the medical privacy rule*. CRS Report for Congress. 14 February 2003.
- Twight C (2002). *Dependent on DC. The rise of Federal control over the lives of ordinary Americans*. Palgrave: St. Martin's Press.
- Varghese J (1982). New legislation gives records management a new importance. *Modern Office* 21(1): 26-28.
- Victorian Government (2001). Second Reading of the Health Records Bill. Hansard, 22 March 2001.
- Wang RY (1998). A product perspective on total data quality management. *Communications of the ACM* 41(2): 58-65.

Appendix: EU Generic Code of Fair Information Principles

This formulation of a code of fair information practices is derived from several sources, including codes developed by the Department of Health, Education, and Welfare (1973), Organization for Economic Cooperation and Development (1980), and Council of Europe (1981).

1. The Principle of Openness

The existence of record-keeping systems and databanks that contain personal data must be publicly known, along with a description of the main purpose and uses of the data.

2. The Principle of Individual Participation

Individuals should have a right to view all information that is collected about them; they must also be able to correct or remove data that is not timely, accurate, relevant, or complete.

3. The Principle of Collection Limitation

There should exist limits to the collection of personal data; data should be collected by lawful and fair means and should be collected, where appropriate, with the knowledge or consent of the subject.

4. The Principle of Data Quality

Personal data should be relevant to the purposes for which it is collected and used; personal data should be accurate, complete, and timely.

5. The Principle of Finality

There should be limits to the use and disclosure of personal data: data should be used only for purposes specified at the time of collection; data should not be otherwise disclosed without the consent of the data subject or other legal authority.

6. The Principle of Security

Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

7. The Principle of Accountability

Record keepers should be accountable for complying with fair information practices.

Reeva Lederman BA, MIS

Lecturer, Department of Information Systems
University of Melbourne
Tel: +61 3 8344 1595
Email: reevaml@unimelb.edu.au

Biographical data

Reeva Lederman has a strong interest in the area of health information systems and has presented related work at significant international conferences, including a presentation on medical data privacy at the IEEE Computer Based Medical Systems Conference in Bethesda, Maryland, in June 2004. Her work has also appeared in the *Health Informatics Journal* and the *Journal of Medical Systems*.