# Managing hospital databases: can large hospitals really protect patient data?

Reeva Lederman

*Health Informatics Journal* 2005 11: 201
DOI: 10.1177/1460458205055685

Health Informatics Journal


Vol 11(3): 201–210 [1460-4582(200509)11:3;201–210; DOI: 10.1177/1460458205055685] www.sagepublications.com

# Managing hospital databases: can large hospitals really protect patient data?

*Reeva Lederman*

**Between 1998 and 2003 a number of European countries, the UK, Canada, Australia and the US all introduced data privacy legislation that sought to comply with the European Data Privacy Directive of 1995 in protecting the privacy of individuals undergoing treatment in large hospitals. In 2004 we find that hospital administrators within these jurisdictions are still struggling to find ways to implement and maintain hospital databases while complying with the given legislation – where compliance seems to require a whole new approach to database management. This research examines the UK Data Protection Act 1998 and considers whether current database management systems allow the EU Directives contained in the Act to be followed in practice. It finds a number of recurrent problems with hospital systems that would make compliance with the Act difficult. These findings have significant implications for hospital information systems development and design.**

## Keywords

data privacy, data quality, information systems design, UK Data Protection Act 1998

## Introduction

Over the last few decades worldwide there has been increased concern and interest in the area of data privacy. Through the 1960s and 1970s interest grew in Western countries in regard to the notion of information privacy, as a general trend toward the collection of large bodies of individual data was observed. Seminal works on privacy such as *Privacy and Freedom* [1] and *The Assault on Privacy* [2] gave rise to new definitions of privacy (e.g. the right of individuals 'to determine for themselves when, how and to what extent

information about them is communicated to others' [1, p. 7]) as concerns about the threat to individual privacy in the electronic age increased. Through the 1970s and 1980s countries such as the UK, Australia, Canada and the US gradually began introducing bodies of legislation dealing with aspects of data protection and freedom of information (e.g. UK Data Protection Act 1984; Victoria Freedom of Information Act 1982), but these tended to be fragmented and non-uniform. In October 1995 the European Union (EU) enacted the Data Privacy Directive [3] following many years of discussion and debate. 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 Data Protection Provisions. These requirements have imposed obligations worldwide in both the business and health sectors.

## *Data protection in the UK*

In Britain, in particular, the NHS Information Strategy of 1998 promoting the development of electronic patient records, developing into the more recently renamed NHS Care Record Service, has raised concerns about access to patients' records [4] where records are integrated across a range of organizations and accessible to increasing numbers of medical personnel.

In the UK, medical data privacy is controlled by both legislation and the common law right to confidentiality. This common law right is not entirely clear, although recent case law suggests that disclosure of de-identified patient data does not constitute a breach of confidentiality [5]. This lack of clarity has been an extra incentive to move to define the law through legislation.

In 1998 the UK Parliament introduced the Data Protection Act (DPA), which supersedes the Data Protection Act 1984 and seeks to comply with the EU Data Privacy Directive. The EU Directive sets down eight data protection principles:

Data

1 must be obtained and processed fairly and lawfully
2 must be held only for the lawful purpose originally collected
3 must be used only for these purposes and disclosed to recognised persons
4 use should be adequate, relevant and not excessive
5 should be accurate and updated
6 should be held no longer than is necessary
7 must be accessible to the individual concerned who has a right to have the information corrected or erased
8 should be secured.

Using these principles the DPA constructs a framework for protecting the privacy, security and confidentiality of medical data, to form a set of legislation which is very similar to that introduced in Australia and the US and a range of European countries. The DPA in particular also aligns itself with the principles of the NHS Code of Conduct which stresses the need to protect patient confidentiality and control over disclosure of information [6].

## *Challenges for the protection of data privacy in hospitals*

The DPA seeks to strike a balance between assuring an individual's health information is protected while allowing the flow of necessary health information. Stevens [7], in a report on similar US legislation (the Medical Privacy Rule), raised the difficulties of achieving these objectives. She criticized the US legislation on the grounds of its complexity, the likely difficulties in compliance, the 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 [8] has suggested that worldwide privacy legislation has been complex and difficult to implement and there has certainly been much criticism of the DPA. Warren et al. [9] claim that 'in order to benefit from the legislation, data subjects need to be well informed and pro-active'. In reality, however, even a proactive subject will not be able to have full access to and control over their medical data where this control is not implemented at the hospital level.

In all large organizations there are difficulties in ensuring control over and quality of organizational data [10, 11] where, at a minimum, good quality data are seen to be accurate, complete and verifiable [12]. 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 [13, 14].

What is striking about the DPA, and similar legislation worldwide, is the extent to which it requires the health providing organization to have control over its patient database in order to ensure appropriate levels of access and distribution of data. For example, under the Act, individuals are entitled to have access to and to be informed about any information about which the individual is the data subject (ch. 29, para. II, 7b), and to be given an opportunity to consent to the disclosure of that information (ch. 29, para. II, 4a), with express refusals of consent to disclosure needing to be considered (ch. 29, para. II, 6d). The DPA speaks expressly of 'fair and lawful' processing of information with an emphasis on whether particular disclosures can reasonably be envisaged [15]. These provisions and many similar ones all require the relevant health provider to exercise complete control over the data it administers and how those data are stored and distributed, and the reliability and quality of the data.

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 [16, 17] where 'healthcare organisations are notorious for huge legacy infrastructures that don't interface' [18]. This results in significantly decreased ability of patients to have access to their full patient record despite this being a primary right under the new legislation. While the press report large sums needing to be invested to implement similar legislation overseas [19], 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 the UK.

Governments worldwide introducing privacy legislation recognized that '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' [20]. However, while it is recognized that there are threats to individual privacy inherent in the use of information technologies, the use of appropriate technology suitably managed can in fact enhance healthcare users' opportunities for privacy protection.

It is argued in this article that to implement the objectives of the Data Protection Act 1998 it will be difficult for health providers to ensure that the data they hold are structured and managed so as to be of high enough quality to provide the full access to and maintenance of accurate records that are 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 the following research questions are considered in this article:

- Do the methods of data management in large hospitals allow these hospitals to satisfy the key EU Data Privacy Directives, as expressed in the legislative requirements of the Data Protection Act 1998, requiring 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?

## Methods

This research involved an initial preliminary study of relevant privacy legislation and literature worldwide, including an extensive review of the DPA. Next, the components of the three issues of privacy, security and confidentiality as expressed in the data protection principles in the legislation were considered, including how they relate to problems of collection and maintenance of records, use and disclosure of patient records, and patients' ability to access and correct their record. A set of interview questions was developed which focused on the approach hospitals were using to ensure compliance with these aspects of the legislation.

The data collection stage of the study involved eight in-depth interviews in hospitals over January and February 2004 with relevant hospital employees, of whom four were health information officers managing a privacy portfolio within the hospital and four 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 selected were in jurisdictions covered by legislation enacted under the EU Data Privacy Directives.

The size of the admissions to the hospitals sampled ranged from approximately 12,000 to 60,000 patients per annum. All of the hospitals provided allied health services including physiotherapy, occupational therapy, social work, nutrition and speech pathology with records showing an average of nearly 2 hours per day being spent by inpatients on allied

health in the public hospitals surveyed. 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 1 hour and were held at the interviewee's workplace and then transcribed and analysed using qualitative data techniques [21].

## Issues of primary significance emerging from the results

The analysis of the data through a grounded theory method [21] revealed four significant issues at all hospital sites that would most impede a hospital's ability to fulfil the requirements of the Data Protection Act 1998:

- the problem of non-integrated databases across hospitals
- the widespread use of paper-based records
- poor security over system data
- poor management of the process of gaining consent to disclosure of patient information.

A sample of the problems arising from these issues is detailed below.

### *Non-integrated 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 and the ability to view the whole patient record to correct them. 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; at another, transplant services were separate; and 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 also 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 decentralized record keeping across the organization'.

At another hospital the central records staff identified significant problems with the maintenance of full test results that also stemmed from the existence of a non-integrated record:

> 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 hospital officers surveyed could guarantee that if a patient made a request for access to their record, the record produced for the individual patient would be a full dataset extracted from all possible repositories.

### *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 hospital's databases. This exposed the record to all forms of privacy violation: it could be improperly used, accidentally disclosed to unauthorized parties, and impossible for the patient to access and correct.

> 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 of 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. 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 re-presents requesting their record or rebooking and we try and find the record and it isn't where we think it is.

Previous research [22] suggests that 'lost' records are commonplace across the medical world and are a significant obstacle to the ability of organizations 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 hard copy 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.

### *Data 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.

> 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 of leaky and unreliable data security and transfer protocols [23]. In many of the hospitals 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:

1. *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 of not just junior staff but also patients accessing files where computers were left unattended.
2. *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, or audit reporting was not implemented. One hospital chose to circumvent its audit process, 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.'
3. *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.
4. *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.

## *Consent to disclosure*

In the hospitals sampled it was found that there were no provisions in the database designs to ensure that any recorded 'consent to disclosure' tags that were implemented were updated. This caused two problems: patients sometimes gave consent when admitted to hospital prior to treatment when they were unaware of what information was about to be collected; alternatively, they refused consent without fully considering that there might be a personal impact from non-disclosure. Hospitals reported situations where confusion over this issue was so great that vital information about patients was not passed on from one hospital to another in an emergency situation where the consent of the individual was not recorded. Those interviewed suggested that some of the difficulty in the consent issue came from the use of field names which did not adequately encapsulate the classes of individuals to which information could be given. While a database might record an individual as 'next of kin', for example, the patient may think of that person as the person who will be told if they die. However, this is not a designation which necessarily covers the full range of persons that the patient is happy to be given information about their medical condition. For example, adult children as well as the spouse might be listed as next of kin.

Consent to disclosure for research purposes is also a problematic issue. When sampled, a large proportion of patients who are asked directly if they consent to the use of data collected from their records for research purposes decline permission for such use [24]. While both schedules 2 and 3 of the DPA require consent to be obtained from the data subject before any information is released to a third party, the NHS has recognized this provision as one with which they have had difficulty in complying [15]. There is a clear need for decision support from information systems and IS design strategies that assist medical and research staff in resolving issues such as whether or not the patient can be identified from the data (when being used for research), whether their consent is express or implied, and whether disclosure is in the public interest or there is a statutory requirement to disclose.

## Discussion

The results of this research suggest that in many large hospitals both computerized and paper-based information is insufficiently integrated and secured to fully protect patient records. Recent press reports suggest that 'health workers are usually acutely aware of the need to maintain patient confidentiality' [25] but the results of this research clearly indicate that the goodwill of staff is not sufficient for genuine compliance with the DPA, or any similar legislation based on the EU information privacy principles.

The results of an unpublished privacy questionnaire at one hospital indicated high levels of satisfaction with the form requirements of privacy implementation. However, the colloquial understanding of privacy by patients (or even hospital staff) can be quite different to the actual legislative requirements. Patients were asked four questions: 'Did you receive privacy information prior to admission?' (70 per cent said yes); 'Was the content of the privacy brochure easy to read?' (78 per cent said yes); 'Did you feel informed on your privacy rights?' (74 per cent said yes); 'Did you feel the collection of your information was done in a fair and non-intrusive way?' (90 per cent 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 is subject to verification and correction.

The motivation for similar legislation in the US recognizes that 'disclosure of personally identifiable health-care information can profoundly affect people's lives' [7] and, as such, aims to give users of the health system control over the data that are held about them. However, this research suggests that many large health organizations are not, in fact, able to give patients this control when the organizations themselves are maintaining fragmented and incomplete patient databases. While hospitals have stated policies which acknowledge the desirability of 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, 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 centralized database. The message for UK hospitals is that, unless management not only implements stricter data collection policies, but also integrates their

functional units sufficiently for a complete and unified patient view to become possible, compliance with the DPA with respect to access to the patient record for appropriate use, disclosure and correction is not feasible.

These findings have important implications for the future development of information systems in hospitals. The implementation of fully integrated databases in tandem with appropriate security controls seems essential for compliance with the DPA. However, in some of the hospitals surveyed, even the minimal security standards evident in organizations that valued their customer data were not implemented. British researchers [23] 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 datasets 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 [26], but this is a challenge that systems developers must be encouraged to meet by hospital management.

## Conclusions

Any legislature attempting to introduce privacy controls faces a number of difficulties: how can privacy be protected while permitting useful research and audit, while presenting minimal risk, harm or offence to the data subject, and while resisting determined third-party interests? The DPA goes some of the way toward dealing with these issues through its provisions covering access, use, disclosure and correction. However, the case studies detailed here make it clear that the methods of data management in large hospitals make compliance with the legislation difficult – an issue not adequately considered when the Act was introduced. Only with fundamental changes to information systems design and administration is genuine compliance with such legislation possible.

If the legislation remains in its current form, health organizations will struggle to comply. Consequently, both legislators and hospital administrators need to take a serious look at the compliance burden being incurred and consider the funding and commitment required for the appropriate information systems development.

## *References*


**1** Westin A F. *Privacy and Freedom*. New York: Atheneum, 1967.
**2** Miller A. *The Assault on Privacy*. Ann Arbor, MI: University of Michigan Press, 1971.
**3** European Commission. *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.* EC/95, 20 February 1995.
**4** Ziebland S, Chappel A, Dumbelow C, Evans J, Prinjha S, Rozmovita L. How the internet affects patients' experience of cancer: a qualitative study. *BMJ* 2004; **328** (6 March).
**5** *Regina* v. *Department of Health, ex parte Source Informatics Ltd*. CA: Simon Brown, Aldous and Schiemann LJJ. 21 December 1999.
**6** NHS. *Code of Conduct for NHS Managers*. http://www.dh.gov.uk/assetRoot/04/08/59/04/04085904.pdf, 10 September 2004.

**7** Stevens G. *A Brief Summary of the Medical Privacy Rule*. CRS Report for Congress. 14 February 2003.
**8** Twight C. *Dependent on D.C.: The Rise of Federal Control over the Lives of Ordinary Americans*. London: Palgrave/St Martin's Press, 2002.
**9** Warren A, Dearnley J, Oppenheim R. Sources of literature on data protection and human rights. *The Journal of Information, Law and Technology* 2001.
**10** Redman T. *Data Quality: The Field Guide*. New Jersey: Digital Press, 2001.
**11** Wang R Y. A product perspective on total data quality management. *Communications of the ACM* 1998; **41** (2); 58–65.
**12** Stair R. *Principles of Information Systems*. Boston: Boyd and Fraser, 1992.
**13** England I. 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, 29–31 July, Canberra*.
**14** Starr P. Smart technology, stunted policy: developing health information networks. *Health Affairs* 1997; **16** (3); 95–105.
**15** Singleton P, Hunnable J, Mason R. *Gaining Patient Consent to Disclosure: A Consultancy Project for the NHS Executive. Report*. 2001.
**16** Bloom F E. Science as a way of life: perplexities of a physician-scientist. *Science* 2003; **300** (5626; 13 June); 1680–5.
**17** Junnakar S. Law prescribes overhaul of aging system. *CNET News.com* 16 June 2003.
**18** Schulten C. Integration architectures in healthcare and how to extend access to mobile healthcare workers. *Proceedings of the Australian Health Informatics Conference 2001, 29–31 July, Canberra*.
**19** Perry J. Medical 'privacy' rule tab $18 billion, value $0. *NewsMax.com* 18 April 2001.
**20** Hansard of the Victorian Parliament, Second Reading of the Health Records Bill, 22 March 2001.
**21** Miles M B, Huberman A M. *Qualitative Data Analysis: An Expanded Source Book* 2nd edn. Thousand Oaks, CA: Sage, 1994.
**22** Lederman R. How poor information systems increase hospital queues. *Health Informatics Journal* 2002; **8**; 147–52.
**23** NHS Lifehouse Project Data Protection Work Team. *Report on Data Usage, Consent, Ethical Approvals and Research Controls.* December 2001.
**24** Baker R, Shiels C, Stevenson K, Fraser R, Stone M. What proportion of patients refuse consent to data collection from their records for research purposes? *British Journal of General Practice* 2000; **50** (457); 655–6.
**25** Place A. Keeping patients' medical records safe from prying eyes. *The Age Newspaper* 12 April 2003; 34.
**26** Flaherty D. Privacy impact assessments: an essential tool for data protection. In *22nd Annual Meeting of Privacy and Data Protection Officials, September 2000, Venice*.



**Correspondence to:** Reeva Lederman

**Reeva Lederman** BA MIS

*Department of Information Systems, University of Melbourne, Victoria 3010, Australia*
*Tel: 61 3 83441535*
*Fax: 61 3 9349 4596*
*E-mail:* reevaml@unimelb.edu.au