Contents

Health Information Management
Vol. 33 (1) 2004

Privacy of health information

Guest Editor: Malcolm Crompton
Associate Editor: Angela Boal
Managing Editor: Dr Lindsay Paul
Editor: Kerin Robinson

President’s Report
• Privacy – it’s your issue
  Angela Randall 2

Guest Editorial
• The privacy imperative for a successful HealthConnect
  Malcolm Crompton
  former Federal Privacy Commissioner 3

Reviewed articles
• Health privacy: the draft Australian National Health Privacy Code and the shared longitudinal electronic health record
  Moira Paterson and Livia Iacovino 5

• The implications of data privacy legislation for the development of hospital information systems
  Reeva Lederman 12

Reports
• HealthConnect: making consent and privacy a priority
  Jane Aitken and Hitendra Gilhotra 18

Professional Practice and Innovation
• Clinical coding audits: an annotated bibliography
  Dianne Williamson 21
The issue of privacy over the past decade has been enhanced through the introduction of legislation, both State and Federal, which has no doubt had an impact on the management of paper-based and electronic health records, and the way in which we ensure data is processed confidentially.

The dilemma has widened with the introduction of electronic health records and access via the Internet to medical records. In the era of area health services and multi-campus health care facilities where the use of a single electronic record is proposed, the belief that our records remain private; while still allowing patient access may be questionable.

How private is private when we are looking at systems such as “HealthConnect” which proposes to create a continuous health record while still allowing access by multi-carers, multi-facilities and the patient? A doctrine expressed through legislation is that patients have not only access, but control over professional access. How will this be managed while still maintaining the integrity of the information contained in the record?

While we give the patient the right of access, and control over permission to view and amend their records, patients of the future will also be able to create, collate, annotate, modify and disseminate records. What will the role of the health information manager of the future be in this era of patient control? Pivotal to the role will be our professional knowledge of the legislation protecting the patient’s privacy, the patient electronic record, and our understanding of the interchange of the records and the technology used to provide it.

The government has recognised the need for a multi-skilled workforce to manage the change and technological advancements of the future. A number of groups and committees have been established to provide professional advice to the Australian Health Information Council and through to the Australian Health Ministers. It is vital that we, as the professional body of the health information management services, are invited to participate in these committees and have sufficient representation on these advisory bodies.

To this end, the HIMAA strategic plan 2004 – 2009 encompasses initiatives for representation on such bodies. In this issue of the journal, our editorial staff have highlighted the issue of privacy in two reviewed articles.

Finally, we welcome the new chair of the Editorial Board, Mrs Kay Bonello. Kay is a senior Health Information Manager with many years of experience, who I am sure will provide excellent guidance to our editorial staff. Also, we welcome Ms Julia Logan from Western Australia as a board member and Associate Editor, and Ms Lindsay Paul as Managing Editor to assist with the production of our journal. Welcome all and we hope your association with the editorial board is very positive.

Angela Randall
President, HIMAA
Tel: +61 2 9887 5001
E-mail: himaa@himaa.org.au
The privacy imperative for a successful HealthConnect

Malcolm Crompton

As part of the Australian Government’s MedicarePlus initiative, a roll-out of the national electronic health records (EHR) system, HealthConnect, is to begin in Tasmania and South Australia from July 2004.

Reflecting the importance placed by the community on the privacy of health information, the Office of the Federal Privacy Commissioner (OFPC) has maintained a strong interest in the development of HealthConnect (see, for example, OFPC 2002). Most recently, in February 2004, the OFPC made a submission to the HealthConnect Project Office on its Interim Research Report and Draft Systems Architecture for HealthConnect (OFPC 2004a). This submission, available from the OFPC’s website at <www.privacy.gov.au>, argues that work remains to be done to ensure adequate privacy protections are in place for HealthConnect.

The potential benefits of well designed, implemented and managed electronic health records systems are difficult to dispute. HealthConnect is conservatively expected to deliver financial savings to the health sector of at least $300 million per year (HealthConnect 2003a), as well as facilitate improved electronic linking of health information for clinical and health research purposes (see, for example, Stanley 2003). Most importantly, it may improve clinical treatment by enhancing information flows between health service providers.

In recognising these potential benefits however, it is essential to pay equal attention to the risks of such a system, including those which might undermine its very success. HealthConnect would vastly increase the capacity to collect, store, copy, transmit, share and manipulate health information, and perhaps in ways not expected by individuals. There is increased potential for health information collected for one purpose to be taken out of context and disclosed for other purposes incrementally less related to the reason for which it was initially collected (the function creep phenomenon, discussed recently in the context of identity management [OFPC 2004b]). This potential is enhanced by the IT-enabled ability to link data from currently disparate sources, possibly including those from beyond the health sector.

If HealthConnect is to meet its objectives, which are partly reliant on achieving a significant critical mass of participants, then it must inspire the trust of the Australian community that personal health information will be kept private. It is axiomatic that individuals’ willingness to engage in the health sector may be affected by their perception of how their personal health information will be used and how much control they have over it. A HealthConnect system that does not engender trust may result in individuals withholding important health information from providers or, in some cases, avoiding medical treatment altogether (Cavoukian 1999; Goldman & Hudson 2000). Accordingly, rather than an obstacle to be mitigated, privacy is a fundamental necessity for an effective EHR system.

Individual control: informed, voluntary choices

Essential to the achievement of trust in individuals is their control over their own information, and this includes choice as to whether they participate in the system at all, and, if they chose to do so, the extent of their participation. The OFPC welcomes the ongoing commitment to informed and voluntary participation in HealthConnect, whereby an individual makes an active decision to opt-in to the system.

However, choice also entails offering options, so that an individual can determine the extent of participation for a given health-service event. In this regard, the Tasmanian fast-track trial does not go quite far enough. In particular, the early evaluation finding that “Consumers are not yet empowered to control the extent to which their information is being shared between participating providers” is of concern (HealthConnect 2003b, p.3).

A more responsive form of consent framework, described as layered-consent, has been proposed by the OFPC. Readers of this journal may recognise this proposal as similar to the model proposed in the UK and known as the sealed envelope. This offers to individuals the choice for particularly sensitive information to be accessible only to nominated providers, who can see the sealed envelope, thus affording a greater degree of control over their information. This would seem to achieve a pragmatic approach to consumer consent without sacrificing adequate choice and control for individuals. An opt-out arrangement is simply not good enough, having the potential to disempower consumers and provide insufficient range of choice.

Accountability and oversight

Also essential in gaining community trust is an accountability and oversight framework, whereby:

- The Australian community is told clearly what the system is intended to do
- The system, once implemented, does what is intended and nothing more or less
- The system operates in an open and accountable way, by way of audit and mandatory reporting, to demonstrate that it is continuing to meet its commitments.

To achieve this, it is necessary that powers regarding the functioning of the system (that is, the management of the system) should be separate from powers of oversight (independent accountability). The oversight body setting the rules for matters such as access and consent arrangements should be separate from a necessary, independent complaints handling body.

System implementation

Two implementation elements that must be addressed prior to HealthConnect roll-out are, first, that a full evaluation must be performed on appropriate, scale-
able trials; and second, robust and reliable identification mechanisms must be established. I strongly oppose appropriating the Medicare number as a HealthConnect identifier, a purpose for which it was not designed and is ill equipped. As I argued in a recent speech, it is essential that we get identity management right (OFPC 2004b); the Medicare number does not achieve this.

Technology and law

Finally, the questions of technology and law warrant attention prior to roll-out. While selecting existing technology has obvious immediate appeal, it is arguable that a system as significant and potentially beneficial as HealthConnect justifies the investment required to explore cutting-edge solutions. Privacy enhancing technologies may offer 21st century alternatives with better outcomes (see, for example, Burkett 1998; Cavoukian 1999). Suitable technologies are being developed; arguments that it is not possible are not valid (OFPC 2004b).

The importance of building privacy into technical design is vital. While law is necessary, including, for example, the still emerging AHMAC National Health Privacy Code, it is largely limited to addressing what should happen, rather than ensuring what can happen. Technology and law are essential co-requisites to a HealthConnect system that can be trusted by the Australian community.

Given the momentum that this project has acquired, it is timely that the privacy implications of such systems are discussed widely, and I applaud the Health Information Management Journal for contributing to this process.

References


Malcolm Crompton
Federal Privacy Commissioner
Office of the Federal Privacy Commissioner
GPO Box 5218
Sydney, NSW 2001
Tel: +61 2 9284 9671
Fax: +61 2 9284 9666

Malcolm Crompton’s term as the Federal Privacy Commissioner expired on 19 April 2004.
Health privacy: the draft Australian national health privacy code and the shared longitudinal electronic health record

Moira Paterson and Livia Iacovino

Abstract
An explicit distinction between shared electronic health records and those at the point of care is required when referring to electronic health records. The former raises particular privacy issues discussed in this paper in relation to HealthConnect and the Draft Australian National Health Privacy Code. In addition to a number of revisions to the code, the analysis recommends that related legislation such as archival and freedom of information law should be reconciled as much as possible within the code, so that a long-term view of the uses, retention and preservation of the longitudinal electronic health record is balanced with privacy, confidentiality and public interest.

Key words: medical records systems; computerised/legislation & jurisprudence; medical record linkage; confidentiality/legislation & jurisprudence; access to information; health information management

Introduction
It is generally accepted that health information has a special quality of sensitivity. This is reflected in the fact that it is almost always listed as one of the categories of information which it is most easy to identify as private (see, for example, Gleeson’s comments in ABC v. Lenah Game Meats (2001) 185 ALR 1.13). As a consequence people are more likely to cooperate with public health strategies if they trust the health system not to act in a way that would undermine their interests and that such trust is undermined by uses of information “in ways that the individual does not expect and has not been consulted about” (Health Issues Centre et al 2002 p. 13; see also Australian Health Ministers’ Advisory Council 2002 p. 7).

In recent years, governments world-wide have encouraged the development of integrated electronic health records regimes which involve the re-use of personal health data in shared networked environments by using personal or entity identifiers coupled with authentication techniques to link personal data across jurisdictions and institutions for online delivery of services (Cornwall 2002). Those regimes pose an increased threat to privacy because their objective is to facilitate the sharing of information and they generally involve the retention of data for the life of the patient.

Magnusson (2002) makes the point that:

As medical records move “on-line” and the centralisation and coordination of health data becomes possible, the demands for third party access, the potential benefits of providing such access, as well as the privacy risks for individual patients, will all increase.

Those developments pose a substantial threat to privacy because of their ability to electronically link and integrate information that was previously segregated within individual health records (Terry 2000). Furthermore, as explained by Carter (1999), an integrated, longitudinal record, once compiled, “is likely to be of interest to many other parties, quite outside those who might be considered to have legitimate public health interests”.

One such initiative, the Australian HealthConnect project, is designed to provide for the collection, storage and exchange of health information on a national basis via the creation of a longitudinal contact record for each patient detailing all interactions with the health system. The government report published in July 2000 (National Electronic Health Records Taskforce 2000), which recommended its development, identified a number of key building blocks as being required to underpin all other activities. These included the development of legal data protection and security frameworks that were regarded as necessary to facilitate electronic transfers and storage of health information (National Electronic Health Records Taskforce 2000). Core components of the policy-design work of HealthConnect include the development of national privacy rules; they also include consent and identification arrangements and a security framework.

To facilitate this task the Australian Health Ministers’ Advisory Council appointed a Privacy Working Group to develop a nationally integrated framework for privacy protection of personal health information. The latter published a Draft Code and an accompanying Discussion Paper (Australian Health Ministers’ Advisory Council 2002) for public consultation in 2002. The latter states that the principles in the Draft Code extend beyond the context of a person’s one-to-one relationship with a health provider to “the exchange of individual health information on a much wider scale between hospitals, pharmacists, other health information providers, health researchers, law enforcement agencies, government departments and individuals” (Australian Health Ministers’ Advisory Council 2002).

This article reports a joint submission made by its authors to the Privacy Working Group in March 2003, which focuses principally on the capacity of the Draft Code to protect health information in a shared longitudinal electronic health record. It also discusses further privacy research in 2004 in relation to the code as expressed in the technical requirements of business processes of HealthConnect.

Scope
Currently, private sector health records are protected by the private sector provisions in the Privacy Act 1988 (Cwlth), except to the extent that they fall within the exception for employee protection. The national
privacy provisions (NPPs) which form the basis for that protection do not distinguish between health information and other types of personal information, although they are given enhanced protection under specific NPPs as a species of sensitive information. Public health sector records are protected under the public sector provisions in the Privacy Act 1988 (Cwlth), the Information Act 2002 (NT) and under sui generis health records laws in Victoria, New South Wales and the ACT, such as the Health Records Act 2001 (Vic), the Health Information Privacy Act 2002 (NSW) and the Health Records (Privacy and Access) Act 1997 (ACT). The latter also protect private records, thereby creating dual protection for private sector health records in those jurisdictions. States other than Victoria and New South Wales do not have either public sector privacy laws or sui generis health records laws. (Public bodies in Queensland, South Australia and Tasmania are, however, subject to the operation of administratively imposed privacy rules. (See www.justice.qld.gov.au/dept/privacy.htm, www.archives.sa.gov.au/privacy/index.html and www.justice.tas.gov.au/legal/privacy/index.htm.) The Draft Code was designed to provide a national framework for the development of consistent state and federal rules for the protection of health information. However, the Discussion Paper leaves open for discussion whether it should be voluntary or compulsory and the extent to which it should apply to health records outside the health sector.

The Discussion Paper suggests three possible options concerning the code’s scope of coverage. The first would limit its application to health services and would have the consequence that personal health information in the possession of bodies other than health services would receive protection only as a species of personal information. This would mean that such health information would receive no protection in those jurisdictions that lack public sector privacy laws. It would also receive no protection under the private sector provisions in the Commonwealth Privacy Act to the extent that it falls within the exception for employee records. There would also be a risk that the restrictions on the transfer of data contained in the code would create difficulties for a health organization wishing to transfer health information to organizations other than health services (Australian Health Ministers’ Advisory Council 2002).

The second option would be to extend the code’s coverage to the handling of all health information no matter where it is held. This would have the consequences that organizations would be required to comply with different privacy standards for health data than for other categories of personal information.

The third option represents a combination of the other two approaches. It envisages that the code would apply primarily to the health sector, with some limited coverage of organisations outside the health sector that might also have significant holdings of health information (Australian Health Ministers’ Advisory Council 2002). There is no information provided concerning the criteria that might be used in determining whether a body has a significant holding of health information.

Arguably, there are two important reasons why a national code should offer mandatory and across-the-board protection. The first is that the unique sensitivity of health information is sufficient to warrant a mandatory and comprehensive approach. The second is that the code will fail to achieve its objective unless such an approach is adopted.

One reason why health information is accepted as being uniquely personal is that our sense of self is intricately bound up with our health status. It is also the case that specific health-related events, such as terminations of pregnancy or the receipt of treatment for a sexually transmitted disease, shed light on other intimate aspects of our lives. A third and related reason is that disclosure of health information may result in adverse consequences for an individual, including discrimination (for example, in the context of employment), or in stigmatisation and social isolation. It should be noted, however, that stigmatisation may not necessarily be reflected in discriminatory action; instead, it may lead to withdrawal of vital social support, thereby having a degenerative effect on the individual’s self esteem (Harris 1997). The risk of adverse consequences is greatest in the case of conditions that involve mental or emotional instability and those which are perceived to be caused by life choices or behaviours (for example the use of illegal drugs or engagement in certain forms of sexual expression) which are not viewed with favour by the general community (Gostin et al 1995). This special sensitivity arises irrespective of the context in which a record is generated or held. Arguably, therefore, health records warrant an individualised treatment that operates across the board, and, in fact, the code as drafted follows the second option.

The stated objectives for the development of the Draft Code specifically include the achievement of national consistency between public and private sectors and across jurisdictions. The lack of a single uniform national framework creates unnecessary complexity for health providers who operate in different jurisdictions or who need to transfer data across different sectors or jurisdictional boundaries. It also creates difficulties for individuals who may receive no protection in some contexts and be required to navigate different and mutually independent review mechanisms.

Although the Discussion Paper provides no explanation of how precisely the Draft Code might contribute to a uniform scheme, one obvious role for it is to serve as model law for those states which currently lack health privacy legislation and as a voluntary private sector code under the Privacy Act. Since the Draft Code draws heavily from the existing sui generis health records laws, this could ultimately result in a regime that is reasonably uniform except in relation to its coverage of health records in the Commonwealth public sector and any records that fall outside the scope of any private sector privacy code. It should be noted in respect of the latter that the exclusion of employee records is currently under review (Commonwealth Attorney-General’s Department 2004). It should, however, also be acknowledged that there are significant differences between existing sui generis laws and between provisions in the draft code and the principles contained in the sui generis laws (see, for example, the submission.
Coverage of HealthConnect

The stated objectives for the development of the Draft Code refer to the need to take into account the initiatives proposed under the HealthConnect network (Australian Health Ministers’ Advisory Council 2002, p. 11). In addition, the Privacy Working Group’s Discussion Paper acknowledges that a robust and consistent privacy framework is needed “...to achieve a viable and secure national health information network that facilitates the exchange of health information between and within health service providers – as proposed under HealthConnect...” (Australian Health Ministers’ Advisory Council 2002, p. 10).

It is currently unclear whether all HealthConnect records will qualify for protection under the private sector provisions in the Commonwealth Privacy Act. That uncertainty arises because of the three levels within its conceptual model: a national coordination layer, a state or area health record system and a provider’s clinical information system (HealthConnect 2003c). Third party access authorisations are within the processes of the health record system that stores the individual’s record at state level. The national level will consolidate into one database all the summaries for secondary and other uses and provide an archival recovery service with archival control at the Commonwealth level (HealthConnect 2003b). Consent information will be held in both the local clinical system and the area or state health record system (HealthConnect 2003a). Therefore, different jurisdictions will be involved from the point of view of the HealthConnect system architecture.

Despite the fact that the code aims to provide rules for networked health systems, it does not make an explicit distinction between shared electronic health records and those at the point of care. The former raises particular privacy and linkage issues. Legislation that also impinges on privacy, including archival and freedom-of-information law, and standards and guidelines should be reconciled as much as possible within the code, so that a long-term view of the uses, retention and preservation of health information and records is balanced with privacy, confidentiality and public interest.

Definitional Issues

Key terms, including health information, health service, and health service provider are defined in Part 4 of the code. However, a definition of a record is also needed. A record, as defined in the International Standards Organisation (ISO) records management standard, is “information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business” (International Standards Organisation 2001, p. 3). The standard includes tracking, which is defined as creating, capturing and maintaining information about the movement and use of records (International Standards Organisation 2001, p. 3).

Tracking provides an auditable trail of record transactions (event histories/audit trails) as part of the record. Consumers require access to information on who saw their health record, what they saw, and when, in particular in the HealthConnect context where secondary uses are extensive. Adding a definition of a record will improve consumers’ rights to a full record and supports the draft national health privacy Principle 5, which deals with access to health information by consumers. This definition would apply to any record, which includes health information.

The definition of organisation is left unclear, as this will depend on the mechanism selected for implementing the code, although there is clear intention that it will include public and private health service providers. This matter requires careful attention as there is confusion when the code switches to responsibilities of an individual health service provider who is defined within the meaning of organisation, and then refers to an organisation which includes more than one health service provider, as well as occasional references to a record keeper. Individuals in an organisation do not register separately to participate in HealthConnect. It is envisaged that “Organisations will manage the access entitlements of the individuals within the organisation and may have a range of clinical and non-clinical users” (HealthConnect 2003d, p. 78). As an organisation may control a large number of users via its own rules, there is a danger that privacy controls may be undermined unless such rules are consistent with the code.

The definition of personal information states that it “does not include information about an individual who has been dead for more than 30 years”. This effectively protects personal information to a length of time applied to medical information in archival legislation. However, access to public health records that are more than 100 years old is commonly provided through archival legislation or practice. For example, the State Records Act 2000 (WA) s. 49 contains a special provision for access to a medical record that is at least one hundred years old that is a State archive (ie, a State record that is to be retained permanently). An alternative approach is to narrow the definition so that it is confined to living persons, which would be consistent with the Commonwealth Privacy Act and most European law; for example, the Personal Data Act 1998 (Sweden), s. 3 defines personal data as “kinds of information that directly or indirectly may be referable to a natural person who is alive”. (See also Australian Health Ministers’ Advisory Council 2002, p. 42).

A final definitional issue relates to the definition of publicly-available health information in cl. 3. Paragraph (c) of that definition refers to “a public record under the control of the Keeper of Public Records” (see also Australian Health Ministers’ Advisory Council 2002, p. 56). The Keeper of Public Records is a term only used in the Public Records Act 1973 (Vic), so there needs to be general wording to cover other public archival authorities throughout Australia. An alternative term could be the relevant public archival authority. Control is also defined differently in different archival legislation, so once again there is a need to provide a more precise meaning.
The adequacy of the NHPPs as a standard for protecting shared electronic health records

The Draft Code covers records in all media, not just those in electronic form, with exemptions only for information collected or held for the purposes of, or in connection with, personal, family or household affairs (Australian Health Ministers’ Advisory Council 2002, p. 66 cl. 1).

As explained above, it is an objective of the Draft Code to enhance HealthConnect and e-health exchange of personal health information between jurisdictions and across health information networks. However, the eleven National Health Privacy Principles (NHPPs) in the Draft Code arguably fail to sufficiently address the unique issues raised by electronic health records, and shared electronic health records in particular. For example, shared records provide access to the whole health history of a patient over his or her lifetime, compiled from a range of individual health records across the health sector. Arguably therefore, NHPP 1.4 (c), which requires that an individual should be made aware of the purposes for which his or her health information is collected, should also require notification of the fact that health information will be shared and the provision of appropriate details concerning any such sharing. Likewise, NHPP 7, which deals with identifiers, and NHPP 9, which deals with trans-border data flows within Australia as well as overseas, should contain provisions that deal expressly with the sharing of records within the context of a shared electronic health record.

Another issue of concern is the matter of security. The electronic storage of data, irrespective of whether or not they are linked for the purposes of access by a multiplicity of persons, increases the potential risks to privacy, but these are magnified by the provision for sharing which is integral to systems such as HealthConnect. Arguably therefore, there is a need for the inclusion of some discussion concerning the appropriate use of privacy enhancing measures such as encryption of messages and virtual private networks via the drafting of suitably worded guidelines which could form the basis for developing requirements in standards governing specifications for shared electronic health systems.

Another important issue relates to the autonomy of patients in determining the range of persons to whom information may be provided and the uses to which it may be put. The draft principles provide that a person’s health information may be used or disclosed for the main reason it was collected, or for another directly related purpose if he or she would reasonably expect this, otherwise further consent is required for its use or disclosure. However, as long as the purpose for collection is made clear there is no limitation as to what it may entail, so that the person may essentially have no choice but to withdraw from the medical consultation, as they may be reluctant to provide the information that is sought.

In the absence of an integrated electronic health records regime, there is scope for flexibility in terms of establishing the uses and disclosures that the patient is willing to accede to and scope for the quarantining of information by consulting different practitioners.

Theoretically, an electronic health records system could be set up so that not only is participation voluntary but also so that participating individuals can decide for themselves on an individual basis precisely which categories of access should apply to each item of information included in their electronic record. Patients may wish to quarantine certain more sensitive types of information; for example, information about a sexually transmitted disease, so that it cannot be accessed by all of the health professionals and administrators who would normally have access to their records. These are implementation issues, which include access permissions that must be built into electronic health systems. Quarantining can be achieved, for example, via the use of passwords and/or alphanumeric identifiers (Schoenbery & Safran 2002). However, in the absence of specific principles requiring such flexibility there is a danger that it may give way to “arguments focusing on clinical necessity, administrative burden and the economic and public health benefits of administrative and research access” (Magnusson 2002). Such principles can, of course, be overridden by legislation, but they have the benefit of requiring Parliament to deal explicitly with the issue.

HealthConnect summaries will be available to primary and secondary user groups. Primary user groups consist of consumers who may wish to review and add to their own health records, and health service providers seeking information about the consumer they are treating. Secondary users are persons and organisations seeking to conduct analysis and research to support several of the objectives set out by the National Electronic Health Records Taskforce. The provision of data for secondary uses will only be allowed under strict protocols requiring the aggregation or de-identification of information and the obtaining of authorisation from a central access authority for the requested use. Secondary users are expected to include researchers (including clinical, health service, administrative, statistical, consumer and epidemiological researchers) seeking information to assist clinical decision making, and managers (including administrators, planners, policy makers and funders) seeking information to assist management decision-making (HealthConnect 2003a, p. 14).

As far as HealthConnect secondary users are concerned, they are all covered in the code under a very wide scope for secondary uses in NHPP 2.2. Although HealthConnect differentiates between secondary uses that are aggregated from those that are de-identified, it recognises that personal information may be inadvertently released regardless of the method of access employed (HealthConnect 2003d, p. 84).

As a minimum, the code should provide that health information cannot be collected for inclusion in an electronic health record without voluntary consent and that inclusion of information within an electronic health record should occur only if the record provides patients with some genuine choice as to its potential uses and disclosure. The current HealthConnect business processes address this by using rules to flag data not available for secondary use (see HealthConnect 2003d, p. 86: “Eliminate those who have indicated that they do not wish their information to be available for the requested secondary use” [Major System Process 4.2]).
Another important issue relates to linkages. A shared electronic health record provides a unique linkage of medical information relating to the treatment of an identifiable individual, which in HealthConnect is envisaged as part of a national identifier database. If it is accepted that participation in a shared electronic health record system should be voluntary, then it follows that there should be limitations imposed on use of unique identifiers which link information contained in that record with information contained in records generated in other contexts. Unless such limitations are imposed, then it may be possible to use the electronic record as the basis for producing a record that is more comprehensive than the record that the patient has agreed to contribute to, thereby substantially undermining patient autonomy. It is therefore imperative that a national code should include provisions that specifically limit linkages without specific consent.

The principle in the Draft Code that deals with identifiers allows an organisation to disclose its own identifier to another organisation without the individual’s consent where this use or disclosure is necessary for it to fulfil its obligations to, or the requirements of the other organisation and does not otherwise contravene NHPP 7.2(a) of the Draft Code. NHPP 7.2(b) also allows for the use and disclosure without consent of an identifier used by another organisation where this is reasonably necessary to fulfil a primary or secondary purpose of collection and does not otherwise contravene the principles. Arguably, what is required in addition is a principle along the lines of HPP 15 of the Health Records and Information Privacy Act 2002 (NSW). This precludes the inclusion of health information in a system that links health records without the individual’s express consent and the disclosure of identifiers for the purpose of allowing for the inclusion of an individual’s health information in such a system.

The appropriateness of requirements concerning the retention of records

Records retention currently depends on legislative and business requirements in different states, including archival legislation. Current state-based record disposal schedules do not adequately cover lifetime healthcare. Although the Draft Code recognises continuing business, legal and research uses in personal health records in NHPP 2.2, the purposes specified do not cover non-medical research of the kind envisaged in archival legislation.

Likewise, NHPP 4, which deals with data security and data retention, applies only in an organisational setting and not in a shared record environment. It proposes that information related to a child can be deleted once the individual attains 25 years, or in any case, 7 years after the last occasion on which a health service was provided to the individual. However, it is unclear whether the seven years applies to discrete data or to the patient’s whole record or history. Some health information may not need to be retained and is covered in disposition schedules issued by archival authorities based on triggers for removing particular types of medical information from the record. In terms of potential litigation, medical practices keep patient records even longer than seven years. Clause 4.2(b) (ii) could instead be redrafted to read “7 years after the last interaction or encounter with the health system”, effectively for the normal expected lifetime of a person, plus 7 years. Alternatively, a longer period could be considered; for example, “30 years after the death of the patient”, which would be consistent with the code’s definition of the end of privacy.

The extent to which an individual should be able to request deletion of health information

NHPP 4 follows the approach in the Health Records Act 2002 (Vic) and the Health Records Act 1997 (ACT) and includes provision for a record found to contain inaccuracies to be held separately from the “active” record in use by the treating team. In the case of the Commonwealth Privacy Act the deletion principle is contained in NPP 10, which regulates the collection of sensitive data. That principle distinguishes between the collection of health information for the purposes of the provision of a health service, which is governed by NPP 10.2, and its collection for other purposes, which is governed by NPP 10.3. Only the latter is subject to NPP 10.4 which requires reasonable steps to be taken to “permanently de-identify” the information before disclosing it.

The question as to whether data should ever be totally deleted (as opposed to being amended or annotated) and the scope of the circumstances in which such a course might be appropriate has previously arisen for consideration in the context of applications for amendment under freedom of information legislation. The Freedom of Information Acts differ in the way in which they deal with data deletion. The Freedom of Information Act 1982 (Vic), for example, implicitly allows for data deletion using controlled authorised destruction by requiring the concurrence of the Keeper of Public Records where a correction or amendment “has the effect of deleting or expunging the information”. At the other extreme, the Freedom of Information Act 1982 (Cwlth), s. 50(3) has been amended so as to preclude deletion.

The general approach taken in Victoria and in those jurisdictions where the position is less clear is that deletion is generally inappropriate. (That approach was endorsed by the New South Wales Court of Appeal in Crewdson v. Central Sydney AHS [2002] NSWCA 345).

In most cases the information privacy rights of individuals can be substantially protected by adding an appropriate amendment or annotation and ensuring that this is provided to any person who accesses or makes use of the information for decision-making purposes. This ensures that individuals are protected from the adverse consequences of decisions based on incorrect data, while preserving the historical integrity of the document. For example, the fact that incorrect data was relied upon may be relevant in the context of litigation for malpractice.

On the other hand, there may be some circumstances where information is demonstrably wrong, and its preservation, even with appropriate corrections or annotations, may result in ongoing harm to the individual whose information has been recorded. In some such cases, the relevant review bodies have required...
total erasure (see, for example, re Foster & Victoria Police (1989) 3 VAR 110). Paragraph 6.7(a) of the code is apparently designed to deal with this contingency. However, it would be preferable to replace the words it is likely with the expression there is a real risk and that this should be supplemented with guidelines which make it clear that the potential harm which must be included includes potential discrimination resulting from the making of decisions which may impact adversely on the individual.

**Issues posed by the interaction between freedom of information legislation and the Draft Code**

Although the Draft Code makes it clear that it is subject to the operation of the Freedom of Information Act, the significance of this fact may be lost on those not familiar with that regime, especially patients. It is therefore vital that there should be specific guidance provided at least by way of guidelines. Persons wishing to exercise access and amendment rights contained in the code need to first of all be aware that public sector bodies are generally subject to freedom of information and that access and amendment rights in respect of personal information, including health records, held by them needs to be exercised via that mechanism.

They also need to be aware that:

- The Commonwealth public sector and the public sectors in each of the Australian states and territories are subject to the operation of Freedom of Information Acts, which, although similar in their basic structure, vary in their details.
- There may also be bodies which would appear to belong within the private sector but which are prescribed bodies for the purposes of freedom of information legislation, for example because they receive government funding.
- Conversely there are a number of public sector bodies or bodies on the periphery of the public sector which are excluded from the operation of freedom of information legislation.
- Freedom of information laws contain rights of access to documents, including health records which may be exercising by persons who are the subject of such records as well as by third parties. They also contain rights of amendment which may be exercised only in relation to the applicant’s own personal information.
- These rights of amendment are dependent on first having obtained access to the document under freedom of information legislation. (A person who has a right of amendment under the code and has not obtained access to the record under freedom of information legislation must therefore exercise this right outside of the freedom of information mechanisms.)
- The rights of access under freedom of information legislation are subject to a number of exemptions, including exemptions designed to protect personal privacy. These differ between freedom of information acts and are not identical to the exemptions in the code.
- There are requirements under freedom of information legislation to consult with persons whose personal information is contained in documents to which access is sought by other persons.
- The freedom of information acts do not deal specifically with capacity, although it has been held that a person who lacks capacity is precluded from making a request for access on their own behalf (see Wallace v. Health Commission of Victoria [1985] VLR 403). As a result, the issue of who has capacity to make a request for access or amendment of a health record may be resolved differently where the application is made under freedom of information legislation.

In summary, there is a need to address the immense complexity of the interaction between the freedom of information and information privacy laws and to provide mechanisms to assist individuals in navigating the system.

**Conclusion**

The HealthConnect Interim Research Report of August 2003 states that the development of core components of policy design work, including specific privacy arrangements, is near completion (HealthConnect 2003b). This is a matter of concern, given that the Privacy Working Group is yet to respond to the various submissions that identified weaknesses in the Draft Code (see, for example, the submission by Privacy New South Wales mentioned previously). Arguably, a national health privacy code that applies to health records that are created from many source systems and that may need to be retained for the lifetime of the patient must take account of the interaction of all relevant legislation to both protect the patient’s privacy and ensure an accurate and reliable record is available for their healthcare. It is our view that more work needs to be done on the Draft Code, and more attention given to the precise mechanisms for its implementation, before this objective can be achieved.

**References**


Acknowledgments

This article draws on research carried out in respect of a project Electronic health records: achieving an effective and ethical legal and record keeping framework funded by an Australian Research Council Discovery Grant, 2002-2004. Administering Institution: Deakin University. Chief Investigators: Associate Professor Danuta Mendelson, School of Law, Deakin University; Dr Livia Iacovino, School of Information Management and Systems, Monash University; Associate Professor Bernadette McSherry and Moira Paterson, Faculty of Law, Monash University.

Moira Paterson BEc, LLB(Hons), LLM (London)
Senior Lecturer and Associate Director of the Centre for Law in a Digital Economy (CLIDE)
Faculty of Law
Monash University

Livia Iacovino BA(Hons), GradDipInfoMan, MA(Archives and Records), PhD
Lecturer and Principal Researcher Records Continuum Research Group
School of Information Management and Systems;
Monash University
Website: www.sims.monash.edu.au/research/rcrg/about/people.html#lv

Contact

Dr Livia Iacovino
School of Information Management and Systems
Monash University
26 Sir John Monash Drive
Caulfield East, VIC 3145
Tel: +61 3 9903 2551
E-mail: Livia.Iacovino@sims.monash.edu.au
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 did 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; and 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 hospitals 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 it is. 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.

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:

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.

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 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? (79% 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


Place A (2003). Keeping patients medical records safe from prying eyes. The Age (Melbourne) 12 April: 2003, p: 34.


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.
HealthConnect: making consent and privacy a priority

Jane Aitken and Hitendra Gilhotra

Introduction

One of the biggest challenges for consumers and health care providers at the point of care is the limited flow of essential health information associated with current health-record-keeping systems. Health care providers generally keep their own patient records, often in a paper-based format. This means that parts of an individual’s health information may be stored in many different locations and can be difficult to access in times of medical need. Even when information is kept in electronic form, it is often scattered across incompatible databases, which inhibits sharing of the information.

Imagine the scene of a car accident on a major highway, in which the unconscious driver, Jane Smith, has been rescued from her wrecked car and lifted into an ambulance. She is about to be sped to hospital in what should be a smooth passage to safety and care. However, this may not necessarily be Jane’s experience. In her unconscious state, she cannot warn the doctors that she is allergic to some medications and cannot take other drugs because of an underlying medical condition. If such crucial information is inaccessible to treating medical staff, potentially fatal errors may result.

Every year, many Australians become ill or die owing to adverse events during diagnosis or treatment because of circumstances, especially in emergency situations, similar to those described in this hypothetical case. It is anticipated that HealthConnect, a cutting-edge national information technology project now under way, will revolutionise the handling of medical records, while dramatically reducing the risk of adverse treatment due to the inaccessibility of health information. HealthConnect is being developed as a partnership between all Australian governments. It will provide an up to the minute, national, Internet-based register of clinically relevant, summarised patient information which will be available to treating doctors and nurses in any location, at any time, subject to the consumer’s consent.

Personal health information is extremely sensitive, however, and consumers must be confident that their information is valued and used wisely. Accordingly, HealthConnect has spent considerable time ensuring that the community’s right to privacy, as well as its interest in achieving better health, is upheld and protected.

This article outlines work under way at the national level to develop HealthConnect and how some of the key issues relating to consumer consent and privacy are being addressed in consultation with key stakeholders.

HealthConnect research and development

The HealthConnect Project was jointly funded by the Australian, State and Territory governments for two years (July 2001 to June 2003), to investigate the feasibility and potential of a national electronic health record network for Australia. At their November 2002 meeting, Australian Health Ministers agreed to a further two-year phase of design and development work, ahead of national implementation of the scheme.

The fundamental purpose of HealthConnect is to collect, store and exchange personal health information, in order to improve the delivery and quality of health care while enhancing the privacy and respecting the dignity of health care consumers. Under HealthConnect, a person’s health-related information will be collected in a standard electronic format at the point of care, such as at a hospital or a general practitioner’s clinic. This information will take the form of health summaries, rather than the complete notes that a health care provider may choose to record in relation to a consultation. Participation in HealthConnect will be voluntary for both consumers and providers. With the consumer’s consent, these summaries will be retrievable at any time they are needed and exchanged via a secure network among those particular health-care providers authorised by the consumer to access this information.

The HealthConnect Project is being undertaken by the HealthConnect Program Office, located in the Australian Government Department of Health and Ageing. Overall governance of the Project is via a joint Australian, State and Territory Government Board. A Stakeholder Reference Group comprising key consumer and provider group representatives has been established to ensure that a wide range of stakeholder views feed into the project.

Substantial progress has been made to date, and the foundations for possible national implementation are now in place. In particular:

- HealthConnect trials in Tasmania (diabetes focus) and Northern Territory (remote and Indigenous focus) have been operating for over 12 months and are showing positive results with strong stakeholder support.
- A North Queensland trial commenced in December 2003, with other trials due to be launched in Brisbane and in two sites in New South Wales in 2004.
- Substantial progress has been made in developing key building blocks, including a national health privacy framework and data, messaging, storage and security standards.
- The HealthConnect Interim Research Report (www.healthconnect.gov.au/researchrep/irr.html), which includes key findings of the value, technical feasibility, building block requirements, costs and sustainability of HealthConnect, has been published.

The Australian Government has also been developing MediConnect, the proposed electronic medication record, which is designed to improve quality and safety in the management of medications by giving
Trialing of consent models


The Northern Territory trial is testing a model in which consumer consent is obtained before the inclusion of an event summary on the HealthConnect record and prior to a provider accessing an individual’s HealthConnect record. The Northern Territory is continuing to test this model for the trial extension from June 2003 to June 2004.

In the Tasmanian trial, the consumer gives standing consent at registration. This spells out what types of information providers are permitted to view on the HealthConnect record. Unless the consumer specifically requests otherwise, all event summaries are automatically included in the HealthConnect record.

The NSW trial (EHR*Net) is testing a model in which consent is obtained at the point of registration, with the capacity to exclude particular individuals from accessing records, or the ability to limit access to only a small number of individuals.

In the North Queensland trial, the consent model uses the participating consumer’s initial consent to participate in the trial to allow nominated practices to have access to the HealthConnect record any time for the consumer’s health care and treatment. This model also uses a standing consent at registration for event summaries being added to HealthConnect. However, providers will also be encouraged to seek verbal consent from the consumer prior to the addition of the summary to the HealthConnect record.

The MediConnect Field Test is testing a consent model which provides consumers with more choices than the HealthConnect models. They include choice about emergency access, restricted access to particular parts of the record, and the consumer’s capacity to add or change information to the record, etc. An important part of the Field Test evaluation will be to assess the workability of these choices in daily practice.

Privacy issues

In addition to the consent issues discussed above, there needs to be in place a robust privacy framework ahead of a national implementation of HealthConnect. The HealthConnect Project is developing a multi-layered approach to privacy. This approach is expected to include legislation and policy rules based on the proposed National Health Privacy Code (Draft National Health Privacy Code, <www.health.gov.au/pubs/nhpcode.htm>) being developed by the National Health Privacy Working Group. The proposed Code sets out a single set of health privacy principles that would apply to the collection, use, disclosure and storage of personal health information held in both the public and private sectors across Australia. There will also be a need for a set of rules and possible legislation for HealthConnect that will set out:
• the uses of data, and the related consent mechanisms;
• national security arrangements for HealthConnect which cover the functions of identification/authentication, access-control mechanisms, message protection, monitoring and detection mechanisms and audit/logging processes; and
• organisational practices, including staff training, which ensure appropriate privacy and security standards are maintained by organisations participating in HealthConnect – as well as ensuring the development of an organisational culture which upholds privacy.

A critical part of the work is to ensure that the proposed privacy framework is developed in close consultation with key stakeholders at all stages. In this way, consumers and providers can help shape HealthConnect so that it meets their needs and engenders trust that health information will be safely handled across the network.

Where to next?
Evidence from the HealthConnect Project and international activity in the area of electronic health records indicates that Australia is on the right track with a national approach. As indicated above, the HealthConnect trials and MediConnect Field Test provide the opportunity to test a range of consent models ahead of national implementation. Building on the work on consent undertaken thus far, the HealthConnect Program Office will be developing a consent framework for HealthConnect drawing on the experiences of the trials and Field Test to date.

A consent working group has also been established by the Australian Health Information Council to consider broader e-health consent issues in 2004. Further policy work on privacy arrangements for HealthConnect is also being undertaken over the next 18 months as part of the pre-implementation work for HealthConnect.

For further information on the HealthConnect Project:
HealthConnect Program Office
MDP 25
Department of Health and Ageing
GPO Box 9848
Canberra ACT 2601
Email: healthconnect@health.gov.au

Dr Jane Aitken
Director
Policy Coordination Section
National e-Health Systems Branch ICD
Department of Health and Ageing
Australian Government

Hitendra Gilhotra
Assistant Director
Policy Coordination Section
National e-Health Systems Branch ICD
Department of Health and Ageing
Australian Government
Clinical coding audits: an annotated bibliography

Dianne Williamson

**Keywords:** accuracy; audit; clinical coding; quality

**Introduction**

The accuracy of clinical morbidity coding is vitally important for all groups who use the resulting databases for the purposes of health services research, allocation of funding, evaluation of health services and clinical interventions, and health services planning (Cornes 1999; Roberts et al 2002). A variety of quality improvement techniques are used to assess the accuracy of clinical morbidity coding, and to introduce changes such as coder and clinician education, clinical documentation, software edits, and coding standards, all of which aim to address issues identified in the accuracy assessment process. Audits are performed by various organisations including health authorities and other funders (such as insurance companies, the Department of Veterans’ Affairs, Transport Accident Commissions), research groups, individual health services, and other agencies with a vested interest in coded data quality (such as the National Centre for Classification in Health, and the Australian Institute of Health and Welfare). These audits include statistical analysis of morbidity databases, using products such as Performance Indicators for Coding Quality, to identify compliance with coding standards, and medical record recoding audits which also assess code selection and sequencing based on medical record content (Reid et al 1999; O’Connell & Perry 2003).

The aim of this project was to identify literature relevant to recoding audits of clinical morbidity data which had been published since the annotated bibliography on data quality was prepared by Chicco in 1997.

**Methodology**

An extensive search for publications on coding quality was undertaken, searching combinations of the terms clinical, coding, ICD, morbidity, data, accuracy, quality, error, and audit. The search involved the online databases of Medline, CINAHL, and PubMed. Google (advanced search) and manual searches of 11 health care journals were also undertaken, in addition to checking the reference lists of identified articles and proceedings of relevant conferences. The search identified 129 published documents related to morbidity coding accuracy for the period January 1997 – April 2004.

Thirty-two of these publications, with a focus on audit methodology or results of morbidity recoding studies, were selected for inclusion in this annotated bibliography. All identified Australian reports have been included, together with a selection of general and condition-specific international recoding studies. Where the same study was reported in more than one publication, only one of these has been included in the annotated bibliography. The articles are presented in alphabetical order by authors’ name.

The common threads of the articles in this bibliography are the quantification of coding differences (or errors) through the process of medical record recoding, the identification of the causes of coding error, and the proposal of strategies for improving coding quality.

**Discussion**

Stated aims vary for each audit, but they generally include assessment of the reliability of coded data for the purposes of funding, evaluation and the planning of health services, in addition to monitoring the health of the population.

This article provides an overview of the methodologies and results of a variety of clinical coding audits, using a methodology that involved recoding medical records. The selection includes audits that have been conducted by auditors who were both internal and external to the organisation that performed the coding function. Some of the audits have sampled the full range of diagnoses and procedures; others focus on a specific specialty area. The terminology used to describe coding accuracy varies between articles, including terms such as inconsistency, error and variation.

The definition of coding inconsistency, and the calculation and description of error, varies between articles and is sometimes not clearly specified. Care should be taken in comparing the results of these audits because of the variations in audit methodology and classification systems, and the terminology, definition and measurement of coding difference.

**Annotated Bibliography**


A recoding audit, focusing on the coding of burns, was conducted in two New South Wales public acute hospitals in 1994 – 1996. A stratified random sample of 300 separations was selected. The aims of the research were to assess compliance with the Australian Coding Standards (ACS), assess the impact of clinical documentation on code allocation, and to identify the change in Diagnosis Related Group (DRG) allocation after recoding. Coding errors were identified in 89% of cases, although there was substantial compliance with ACS. After recoding, DRG allocation changed in 9% of cases. Several documentation issues were noted, including variation between multiple burns charts; variation between burns charts and narrative descriptions; and lack of specific documentation regarding site, thickness and extent. In 46% of cases with an error in the coding of site or thickness of burn the clinical
documentation was noted to be inconsistent or unclear. Other factors that may have impacted on the error rate were the clinical complexity and relative rarity of burns cases. In addition to recommendations on coding standards and coding practice, the authors suggested that documentation could be improved by the implementation of standardised burns charts and clinical terminology, and education of clinicians on the importance of detailed and consistent documentation.

American Health Information Management Association Coding Products and Services Team (2003). Managing and improving data quality (Updated) (AHIMA Practice Brief). *Journal of the American Health Information Management Association* 74(7): 64A-C.

This document is one of a series of practice guidelines produced by the American Health Information Management Association, updating the 1996 version. Accurate reporting of clinical codes is described as an activity requiring active collaboration of health information managers, information technology, clinical and business staff; however, the document indicates that the overall responsibility for data quality should reside with the health information service. The guidelines include initiatives and recommendations for data quality management, several of which relate to internal audits, including, but not limited to, clinical coding: review of code selection, review of software which may generate codes, and review of medical record forms or other means used to collect data. Other recommendations include physician review of code allocation, continuing education programs for clinicians and coders, improvement of clinical documentation, and coding from the entire clinical record.


The focus of the introduction of this article is the financial consequences of incorrect code, and therefore incorrect DRG, allocation. The author then describes an ideal coding compliance program, comprising five components, which enhances coding quality to avoid false claims. The detection component proposes computer software to audit 100% of cases for clinical consistency, compliance with data submission requirements, and unusual resource matches (such as short length of stay matched to acute myocardial infarction or assisted ventilation). The correction component involves recoding records with potential non-compliance identified by the detection software, with correction of codes as appropriate. The prevention component evolves from the reports of the detection software that provide a text description to explain the reason for the potential non-compliance. The verification component involves the development of a coding compliance database to track code-error detection and code amendments, providing both an audit trail and a basis for error analysis. Comparison is the final component of the proposed program and includes review of coding practice, using the coding compliance database, to monitor performance within the organisation and to be used as the basis of benchmarking with other agencies. The proposed program has the potential of being labour intensive, but would increase coding effectiveness and efficiency in the long term. The article also discusses the advantages and disadvantages of coder self-audit compared to audit by an independent auditor.


The author describes several programs that are designed to improve the quality of reported coded data. These include a state health authority system of computer edits, a hospital association recoding audit, and a concurrent coding project. The first program described is a set of software edits used by the State of California to check all coded data submitted by hospitals for completeness and compliance with published coding rules, conventions and guidelines. Error reports are then provided to hospitals so that data can be checked and resubmitted to correct the identified errors. The second program, conducted by the New Jersey Hospital Association, has been reviewing coded data for 25 years. Results of a large 1996 audit involved the identification of coding errors using specialised software. The most common error types identified were omission of comorbidity and complication codes for recorded conditions, unclear or insufficient physician documentation, and incorrect selection or sequencing of principal diagnosis. The third program to be described involves daily review of current inpatient records by a health information manager to identify the potential DRG allocation, and inadequate documentation, such as conditions that have been treated but not formally documented. As a result, the Health Information Manager works closely with the case manager and clinicians during the inpatient stay to improve the content of the medical records and clinician understanding of the impact on DRG allocation.


This article describes key elements of a process for conducting internal coding audits and monitoring coding for potential non-compliance with coding standards. The author recommends that the audit process be formally documented and reported, and that it becomes a regular component of the function of the Health Information Service. Criteria for selection of auditors are specified as competence, experience, knowledge of reimbursement systems, and involvement in continuing education activities. A variety of record-sampling strategies are described. The article lists common coding errors and causes and makes recommendations for analysis, reporting, and corrective action.

A variety of activities were implemented in an Australian public metropolitan teaching hospital to demonstrate the application of a Continuous Quality Improvement Model (CQIM) to several aspects of the coding function. One of these activities involved an internal recoding audit, using a sample of 50 surgical discharges, to measure coding accuracy before and after the introduction of the CQIM. The number and source of coding errors was analysed to identify areas in which improvements could be achieved. Results indicated a substantial improvement in coding quality in the second audit, although the authors note that the sample size and other confounding factors may have had an impact on this outcome. The authors recommended that CQIM, including coding audit activities, could be an effective process for achieving improvements in the coding function.


This article reviews the published results of 21 recording audits performed in England, Northern Ireland, Scotland and Wales during the period 1975-1998. Sample sizes varied from 19 to 9,416 records, and many of the audits were focused on specific conditions or procedures. The larger audits were conducted on Scottish Morbidity Record (SMR) data. Coding accuracy rates for diagnoses, using the International Classification of Diseases (ICD), and procedures, using the Classification of Surgical Procedures and Operations (OPCS), varied from 53% to 100%. Several confounding factors which make it difficult to compare accuracy measures and rates are identified, including auditors having access to additional information added to the record post-discharge changes in classification systems and changes in coder training and support systems. The authors suggest the need for additional and more extensive audits and research into methods of improving coding accuracy.


This American recoding audit focused on 40 randomly selected records of patients who had undergone spinal surgery. Although the accuracy of individual codes was identified as 95%, overall the researchers found that in 70% of cases lacking or inaccurate data were reported. One of the major causes of this inaccuracy was documentation where not all procedures performed had been recorded in the medical record, or procedures were recorded sequentially (ie, in order of completion) rather than in order of significance or severity. The availability of International Classification of diseases, 9th revision, Clinical Modification (ICD-9-CM) codes to adequately describe the procedures was also criticised. Although this was a small study, it clearly demonstrated the importance of clinical documentation. The authors concluded that education of physicians and coders was an essential factor in improving coding quality for purposes such as resource allocation.


This annotated bibliography comprises commentaries on 66 publications relating to the quality of coded clinical data, published during the period 1978-1997. Fourteen of the items contain information about recoding audits.


The study reported in this article highlighted the impact of clinical documentation on accurate code allocation. The research team recoded 100 records of trauma patients admitted over a two-month period in 2000 from the trauma centre of a metropolitan hospital. The recoding process included a review of the Trauma Case Manager Record for these patients, resulting in additional codes for 74% of records, based on the additional information from this source. Recoding changed the DRG allocation in 28% of cases. Involvement of nursing case managers to review documentation and coding, in addition to managing patients with complex conditions, is proposed as a method of improving coding accuracy, funding, and patient care.


This article reports the methodology and results of a recoding audit conducted at two large, acute health services in England where records had been coded using the ICD and OPCS. A stratified random sample of 1,607 episodes was selected for general conditions and four specific diagnosis groups (asthma, diabetes, fractured femur, and appendicitis with appendectomy). Records were recoded, blind, by external auditors who were experienced clinical coders. Accuracy measures identified “exact” and “approximate” (to three-digit code level) matches for the principal diagnosis and procedure codes. Results were also analysed to assess difference in DRG allocation. The lowest rate of exact code match was with coding of diabetes as the principal condition. The agreement for exact match of principal diagnosis codes varied from 6% to 65%. Categories of disagreements over codes included difference in selection of principal diagnosis, coding of symptoms, specificity of code selection, incorrect diagnosis selection, and omitted codes for secondary codes and co-morbidities. The researchers queried the validity of code selection by the external auditors, and whether they may have accessed material added to the medical record after the original coding had been performed. The authors also commented on the impact of poor medical record documentation on code accuracy and the responsibility of clinicians in this re-
Recommendations were made for regular audits of medical record content, in addition to coding audits.


Concurrent auditing, or checking coding accuracy prior to reporting for reimbursement purposes, is recommended as best practice by the author. This concurrent process may be achieved by use of editing software that identifies records that should be reviewed and recoded as appropriate. Trending is described as an important complementary retrospective coding audit process. This can be achieved by comparing activity at 6- or 12-month intervals to identify changes in diagnostic or coding practice. As an example, changes in code allocation over a 12-month period are presented for the diagnoses of transient ischaemic attack and cerebrovascular accident, with an analysis of number of patients and average length of stay. Retrospective review of cases coded to “other specified” codes is also recommended.


The American Office of the Inspector General (OIG) recommends that health care agencies perform regular internal coding audits; however, the author of this article claims that their guidelines do not provide adequate advice on methodology. This article attempts to meet this need by briefly discussing the methodological issues of sample size, sample selection, and audit frequency.


The author emphasises the potential financial impact of inaccurate DRG allocation; over-coding may result in penalties and fines in the US healthcare environment, and under-coding may result in less than optimal reimbursement. The process of assessing coding compliance is described, including policy development and implementation, medical record review, claims review, and staff interviews to review education and resource needs. Instructions for conducting coding audits, including sample worksheets, are provided. Feedback of results, staff training, and on-going monitoring processes are described as key components of the coding compliance program.


This paper describes the Australian Coding Benchmark Audit (ACBA) as a tool for uniformly undertaking recoding audits and recording and analysing the results. ACBA classifies the type and cause of errors and distinguishes “coder errors” from “system errors” to facilitate the development of quality management activities to improve coding accuracy. Issues of auditor selection and frequency of coding audits are discussed. Tools for recording and analysing audit results, and reporting these for internal feedback and external benchmarking purposes, are described.


The importance of careful selection of external coding consultants and auditors is discussed in this article. The author presents an extensive list of criteria for the selection of auditing companies that could also be applied to individual coding consultants. Criteria relating to the auditors include auditor experience, appropriate education, involvement in continuing education activities, provision of references, and fee structure. Other auditor selection criteria are based on processes used by the auditor, such as use of appropriate standards; review of all coding errors, not only those which impact on DRG assignment; and providing documented justification for coding discrepancies by referring to published standards.


This article describes a process of developing a coding compliance program in 13 steps. Several of the steps relate to the planning, conduct and follow-up of coding audit procedures. Audit issues discussed by the author are determination of audit focus, timing of audit (concurrent or retrospective), sample selection, sample size, selection of auditor (internal or external), review of results by a committee, and development of strategies to improve identified coding problems.


The focus of this Tasmanian audit was at the District Hospital level, where the practice was for front sheets from medical records to be sent to a major acute care hospital for coding. Eight of the 16 District Hospitals were included in the audit of 172 episodes of care; the auditors recoded at these hospitals using the medical records. A change in principal diagnosis was noted in 29.65% of episodes, and a change of DRG allocation resulted in 29.91% of episodes. The most common types of errors were attributed to front sheet documentation issues, including principal diagnosis not in accordance with ACS, additional diagnoses and procedures not recorded, and less specific information than recorded elsewhere in the medical record. Issues with identification of qualified or unqualified newborns were also noted. As a result of the study it was recommended that qualified coders visit the District Hospitals to code, on site, from the entire medical record, and that a range of clinician education activities be introduced to increase awareness of documentation requirements.
The focus of this review was the records of 1109 day-procedure patients treated in a urology department over a one-year period in 1999–2000. The study compared the content of the two databases maintained by the Urology Department and the English hospital in which it was located. In addition to coding variance and coding errors, the researchers identified a large discrepancy between the number of patients in the databases; 480 of the cases in the departmental database were not present in the hospital database. The cause of coding errors was identified as lack of coder knowledge of surgical procedures, coder reluctance to code more than one procedure, and poor clinical documentation. Interestingly, the recommendations to reduce future error include the suggestion that coders code from the discharge summary instead of reading the medical record.


The results of an American Association of Health Information Management (AHIMA) survey on productivity measures used in United States health care agencies are presented in this article. Survey respondents self-reported coding error rates based on performance measures of the number of claims for reimbursement returned (due to missing support documentation, coding errors, or wrong DRG assignment). 87% of respondents indicated that less than 5% of their records had significant coding error.


In this article the authors provide an extensive description of the compliance programs introduced for health care agencies in the United States to improve coding quality through reductions in false or excessive claims for reimbursement. The authors also report on a national survey of over 16,000 health information managers who identified the extent of external audits conducted by the Health Care Financing Administration (HCFA) or State authorities in the previous two-year period. 13.2% of respondents indicated an incidence of recent state audit or investigation, with medium-sized inpatient facilities most likely to be targeted. HCFA audits were reported by 16.1% of respondents, with medium- to large-sized inpatient facilities most likely to be targeted. In conclusion, the authors emphasise the importance of internal compliance programs in relation to coding quality.

The research reported in this article focused on the coding of complications, based on a medical record review. A sample of 485 cases were selected, based on Medicare hospital discharge data from 1994 for California and Connecticut. Auditors established whether the documentation in the medical record supported the code allocation by containing objective physical evidence of the complication, containing physicians’ notes relating to the complication but without objective evidence, or containing no evidence of the complication. A surprising number of medical records contained no evidence of the coded complication: 19.4% of surgical cases, and 29.9% of medical cases. The following conditions were coded most frequently without documented evidence: post-operative wound infection 36.6%; deep vein thrombosis and pulmonary embolism in medical cases 33.3%; deep vein thrombosis and pulmonary embolism in surgical cases 25%; and post-procedural haemorrhage or haematoma in medical cases 26.7%. The authors note limitations of their study, but raise concerns about external monitoring of hospital performance based on data that they conclude have questionable clinical validity.


The authors conducted a secondary analysis of data collected in the process of a 1993-1994 recoding audit of 7,013 records from 63 Victorian hospitals. The purpose of the analysis was to identify the validity of data in the Victorian Inpatient Minimum Database (VIMD) for epidemiological studies, disease surveillance, and other research purposes. The analysis identified a change in DRG assignment in 13.6% of separations, and a change of principal diagnosis in 22% of separations. Higher rates of coding discrepancy were found in rarer DRGs, medical DRGs, complex cases with a large number of codes, and rural hospitals. In conclusion, the authors stated that the VIMD was a reliable and relatively accurate source of data for epidemiological studies, where researchers were aware of the strengths and limitations of the data.


This article reports the results of a coding validation study of 546 Victorian public hospital separations in 1994–1995 with a principal diagnosis code of 800–999 and a cause-of-injury code. Following the recoding process, error rates for both principal diagnosis and cause of injury were calculated, and grouped as omission of code, superfluous code, discrepancy of allocated code, and change in code sequence. 94% of code discrepancy in the principal diagnosis code related to different selection of codes within the same group of codes, and approximately half of these were minor changes at the level of the last two digits. The Victorian coding error rates for complications of medical and surgical care were noted to be low in compari-

This paper presents an overview of the objectives, methodology and results of audits conducted on data submitted to the VIMD for the period 1998–1999. The audit involved recoding a sample of 7,004 records from 50 hospitals, in addition to checking several administrative and demographic data items which may impact on DRG allocation. The auditors also reported on coding infrastructure issues which may impact on coding accuracy and timeliness of reporting to the Department of Human Services. Results were analysed to enable comparisons between Major Diagnostic Categories, hospital groups, and between metropolitan and rural locations. 13.05% of cases recoded resulted in a change of DRG. Reasons for differences in coding were identified, and the categories which had the highest rates of coding inconsistency were “incorrect code assigned for the condition/procedure”, 24%; and “hospital’s code not necessary or not justified by documentation”, 20%. The paper concludes with an extensive list of recommendations.


The aim of this project was to identify the coding accuracy of patients treated for endophthalmitis in Western Australian hospitals for the extensive period 1980–1998. In addition to recoding cases from the Hospital Morbidity Data System (HMDS), other sources, including surgeons’ logbooks and microbiology and anaesthetic databases, were compared to the HMDS. These supplementary sources identified cases which had been omitted from the HMDS, or which were present but not coded as endophthalmitis. Incorrect coding was attributed to misunderstanding of eye infections, and the misleading structure and index of 1980s editions of coding books. Coding accuracy was noted as having improved since the 1980s, and this was attributed to coder education and improvements in classification systems.


This paper describes the Department of Health (Western Australia) program of recoding audits conducted at eight hospitals in the period 1998 to 2001. An initial random sample of 1,152 records was audited, followed by a targeted audit of 542 records focusing on DRGs identified as having high error rates in the random audit. Results of these audits indicated the four major types of error to be principal diagnosis, omissions (undercoding), failure to follow index (coding conventions), and overcoding of additional diagnosis. The author discusses problems with the coding of principal diagnosis and additional diagnoses, which were commonly related to misinterpretation of the relevant coding standards ACS0001 and ACS0002. Disparate diabetes coding practice prior to the introduction of the third edition changes is also noted. The value of targeted audits, and subsequent targeted coder educational activities, is discussed.


A three-stage coding audit program has been developed by Northwestern Health, a network of Victorian metropolitan public hospitals. Primary audits comprise several auditing techniques, including review of 100% of cases where there is a high financial risk to the hospital (eg, high-cost procedures, ventilation and outliers) and recoding of a sample of cases from a specialty for educational purposes, including “round table” comparisons. Secondary audits use the ACBA methodology, sampling 5% of separations for three months of the year. Tertiary audits are those conducted by external funding agencies, including private health insurance companies and the DHS. The process of reporting results and implementation of recommendations following each audit are discussed. The outcomes of this comprehensive auditing program are identified as improved data integrity, staffing flexibility across the network, support for coders previously isolated in smaller hospitals, and enhancement of the profile of the clinical coder.


This article describes five levels of activity that comprise the program used by an American hospital to optimise clinical coding accuracy. The fourth, review, level involves quarterly internal coding audits, conducted by senior coding staff, on a stratified sample of 10% of records for each coder. The audit checks for accuracy of abstraction, code selection, code sequencing, and DRG assignment. A weighted scoring system is used based on the type and impact of coding error. A higher weighting is applied where the coding error impacts on DRG allocation. Coders are expected to maintain a minimum of 93% accuracy. A review of coders with high error rates is conducted one month following discussion and coder education, and coders face disciplinary action, including dismissal, if minimum accuracy rates are not maintained.

The accuracy of coded data submitted to the Western Australian Hospital Morbidity Data System in 1996–1997 was measured in a recoding audit of two public and five private hospitals. A sample of 1,050 cases was selected randomly, although some cases of high complexity were also included. Records were recoded “blind” by external auditors and code differences were discussed with the original coders, and checked by the senior auditor. Coder characteristics, including scope and length of experience, were noted by the auditors. Inaccurate coding was analysed to identify an overall 13.2% change of DRG assignment, with individual hospital accuracy results ranging from 82% to 94.5%. Four major types of coding problem were identified: incorrect abstraction, 36%; inaccurate code assignment, 33%; non-application of the ACS, 14%; and poor documentation, 7%. There is substantial discussion on the cause of the coding problems, including incomplete clinical documentation, and inadequate coder knowledge of ACS changes.


The authors describe the responsibilities of the position of Coding Quality Analyst at an American hospital. This includes the development, in conjunction with coding staff, of an annual plan of monthly coding audit activities. These audits are focused on cases which are either high risk (impact on reimbursement), high volume, and special interest (such as new procedures). A database of audit results includes individual coder performance and is used to identify education needs and other strategies for improving coding accuracy. In addition to monthly audits conducted by the Coding Quality Analyst, external auditors are used to validate the hospital’s review processes.


This paper provides an analysis of results of 47 ACBA audits conducted in 30 Australian hospitals over a 12-month period, and submitted to the NCCH for benchmarking purposes. The 12-month time period and the sample size (3,912 medical records) was noted to be too small for meaningful trend analysis of error rates; however, it is noted that this standardised audit method has significant potential for tracking improvements over time, and for individual hospitals to benchmark their performance to nationally reported results. Hospitals also provided useful feedback on the auditing process to NCCH for consideration in further development of the ACBA tool.

### Additional references


**Dianne Williamson** BAppSc (MRA), GDipErg

Project Officer
National Centre for Classification in Health
School of Public Health
La Trobe University
Bundoora, VIC
Tel: +61 3 9479 1135
E-mail: d.williamson@latrobe.edu.au

Correspondence to Dianne Williamson

This article was completed whilst Dianne was on secondment to the National Centre for Classification in Health.