electronic Journal of Health Informatics
www.eJHI.net
2012; Vol 7(2):e19

Practical Measures for Keeping Health Information Private

Roderick Neame

University of Queensland, Brisbane, Queensland, Australia

Abstract

Increasingly large amounts of personal information are being captured and stored within healthcare systems; and these data are being shared increasingly widely, and aggregated into ever larger data warehouses. There are good and proper reasons for doing this and the end result will bring benefits to physicians, patients and the community. However there are also demands for health information, for unethical and illegal purposes, and the evidence indicates that there is a ready supply line for it; on the other hand there may be little need to use that supply line when such vast quantities of personalised health information are regularly being lost or otherwise disclosed by government and private sector organisations.

This article takes a careful look at information privacy to determine where and how personal information is being abused and disclosed, and how to prevent this. Some of the disclosures are simply a consequence of laziness and carelessness; others are calculating and deliberate; but they can all be controlled and in some cases eliminated by applying well-established methods and technology. The problem seems to be that institutions either do not understand what is required of them, or do not care enough to implement the appropriate measures. It seems also that systems are not being planned with privacy in mind, and consequently are not readily able to accommodate these demands.

Keywords: Health Information Privacy; Unique Identifiers; Network Infrastructures

1 Introduction

Patients expect that the healthcare system will keep their personal care records secret. Arguments have been put forward that privacy of health information is only an issue of concern for those with something to hide. Whether or not this is true, the evidence suggests the issue is a priority for a large part of the population[1,2], and patients are unwilling to tell the whole truth about certain health matters where they feel their information may not be kept private, so making the task of care providers more difficult and risky. This aligns with the ethical principle of personal autonomy, which recognises the right of the patient to control all matters relating to their own body, including information about it. Medicine has a long history of ethics going back to the oath of Hippocrates[3], which includes the requirement to keep secret information that is shared with a clinician in a consultation. Many professional associations require their members to keep such confidences, and many hold the power to censure or de-register their members whose ethical conduct fails to match up to expectations, even if they have not actually committed a legal offence.

Public anxiety about information privacy is high, especially as a consequence of the almost daily losses of personal information from both private and government records, the statistics of which are quite frightening[4]: disclosed reports detail over 120 million records that were affected in 2011, with almost one third of the incidents occurring in the health sector; how much this would be increased by inclusion of undisclosed losses is anyone's guess. There is undoubtedly a strong demand for personal information of all types, including health information[eg 5], and the system of data protection is potentially flawed[eg 6,7].

Issues relating to information privacy and system

security are crucial issues in the context of information management systems: trust is hard won and loss of trust can be extremely damaging[8] especially where such sensitive information as that recorded for healthcare is involved. Failure to manage these effectively can cause loss of confidence and bring major information systems to their knees unless users (public and professionals alike) are assured of the highest level of integrity and privacy protection.

The legal system recognises the personal autonomy principle, and requires that the patient is given the right to control what happens to their bodies and to their personal information: every action and intervention relating to these matters must be the subject of a valid and informed legal consent process. Whilst consent may be implied and valid, the weakness is that this depends totally on who is making that implication and whether or not it aligns with the patients intentions. There are two relevant bodies of law in UK: one is the Human rights Act (1998), in which article 8 guarantees that the State shall not interfere with the privacy of individual; the other is the Data Protection Act (1998) which places numerous obligations on those who are custodians of personal information in respect of all processes in the information cycle (data collection, storage, access, use, disclosure, destruction etc). It is a specific obligation that custodians of personal information keep personal information secure and protected from any unauthorised access. Equivalent legislation exists in most other developed countries, and it seems reasonable to suppose that a roughly equivalent arrangement should be the basis of systems planning worldwide, not simply based on ethics. Being a signatory to the Universal Declaration of Human Rights (1948), Australia supports the issues, although it lacks a Human Rights Act: however it does have a Privacy Act[9].

There are numerous legitimate uses for which health information is required: authorisation to access it and the terms and conditions of that access thus becomes a vital issue. In terms of the ethical principle of personal autonomy, the only legitimate day-to-day source of authority to access records where the subject is identified is the patient[10,11], whether or not their physician may believe that refusing permission to disclose personalised information (eg to a colleague) is wise. However confidentiality is not absolute: there are various exceptional circumstances recognised, such as where access is permitted by statute, by court order, or where there is a real belief that disclosure is necessary to prevent a crime or the risk of serious damage or injury, or where there is an overriding issue of public interest. The law recognises the personal autonomy principle as of central and guiding importance in the form of data protection Acts and associated privacy principles[eg 12,13]. In the exceptional event that the patient appears incapable of giving valid consent to access their records (eg through incapacity, confusion, lack of comprehension, inability to reason etc), the attending clinician may take whatever steps are believed necessary in the context of solving the immediate health problem, including accessing/disclosing information as well as undertaking interventions, without patient authority under the legal doctrine of the 'best interests' of the patient.

For clarity there follow (below) a number of working definitions of concepts used in this article with which general readers may not be familiar:

- *Private:* the right of a person to control who knows what about them, and to reveal themselves, and particularly that information which they consider sensitive, selectively and at a time, place and manner of their choosing,
- *Confidentiality:* an ethical principle (and in some instances, including medicine, a legal requirement) to keep information divulged by one person to another within a tightly restricted environment and to prevent it becoming public knowledge
- *Security:* keeping information available to authorised users, ensuring it is neither lost or corrupted, and protecting it from all forms of attack, and particularly access by unauthorised persons
- *Primary use:* the primary use of healthcare information is in the context of the care services provided to the patient, now and in the future, including such associated but necessary administrative functions as audit, quality assurance and accounting
- *Secondary use:* the secondary uses of health information include all those uses that are not directly related to the care of the individual, including research, public health studies, data warehousing, business management, manpower and facilities planning, statistical returns etc
- *Personalised information:* care information which is associated with personally identifying data which is sufficient for a third party (eg analyst) to be able to identify the person concerned, the information is 'personalised': where re-identification is impossible the information is 'de-personalised' or 'de-identified'.

This article refers at various points to issues of ethics and the law. Medical ethics have no geographic limit to

their application, but the law does recognise different jurisdictions. In this article reference is generally made to Australian and UK laws, but equivalent legislation exists in almost every developed nation.

2 Uses of Health Information

A century ago there was just one purpose for making and keeping health records: that was to act as an aide memoire to the physician (primary user) as to what was the patient problem and how it was progressing, and to calculate the account for payment by the patient. Although this primary function of medical records remains unchanged, since that time the uses to which health information from personal care records is put have expanded considerably, including insurers and payors, administrators and business managers, finance officers, auditors, referral services, nurses, clinic/ward clerks, technicians, clinicians and so on.

Some of these parties (eg other clinicians and auditors) may need access to the full details in the patient record, and this disclosure may require the authorisation of the patient (see above). Most of the rest do not need access to the full records of the care event, but their needs can be served with abstracts – eg unique identity, service date(s), diagnosis(es) or reasons for encounter, services provided (translates to billable event(s)), service provider/clinic etc. These details are quite sufficient to enable the event(s) to be administratively verified and accounted for, and for an invoice to be raised and reconciled with the payment when received from the payor: this also serves to preserve patient privacy. However the current typical arrangement is that almost anyone in the care enterprise has access to the full records of care for all patients, irrespective of their needs: alternate views in which only an abstract of the record appropriate to the specific data needs of that user are not generally available. This almost universal practice demonstrates either a scant regard for the law relating to personal information privacy on the part of the users/institution, or a failure to comprehend its provisions on the part of both systems developer/vendor and users/institution. There is data from several other sources to supporting the notion that healthcare professionals and institutions are either ignorant or careless as regards privacy issues – not least the catalogue of recorded and entirely avoidable data losses[14], as well as specific studies showing evidence that privacy practices amongst some of those with custodianship of confidential electronic medical records are less than adequate[15].

As an extension to enable records to better serve the primary purposes, there is considerable interest and potential to benefit clinicians and patients alike through bringing together all the events and encounters for an individual into a longitudinal record of care, thereby creating a single repository that could in principle chart the health-related events for an individual from 'cradle to grave'. Such a repository could be of considerable benefit to the patient, but access to it would clearly need to be under the control of the individual, who should also have the ability to control who sees which parts of the whole.

Moving on to the secondary (ie not directly linked to the care of the patient) uses of healthcare records, these extend to the wider interests of public health and research. There is a fast growing and potentially intrusive demand for care information to bring records together into data warehouses in order to analyse, search and summarise them for new insights into incidences, causation, natural history, treatments and outcomes. These analyses will throw new light on trends, data linkages/associations, new syndromes, treatment risks (eg associated with devices, medicines, procedures), diagnostic pathways, best quality care practices, costs, quality of life etc which will be invaluable in informing clinicians and patients of the options and statistics relating to their situation. These data can be formulated into knowledgebases, which are becoming of considerable interest for development of artificially intelligent clinical decision support systems, and to contain costs, manage risks and get the best possible value for every health dollar spent. None of these purposes requires the actual identity of the individual to be disclosed: the data can be anonymised with all personal identifiers removed. However anonymisation does impeded some longitudinal studies where following the same patient over time is required, in which case the data may be pseudonymised where personal identifiers are replaced with a cipher, but the cipher remains always the same for that individual so permitting longitudinal record linking.

3 The Privacy Challenge

The issue with information management systems is that they are designed to achieve specific purposes, and those purposes are deeply embedded in the way the systems are built and operate 'behind the scenes'. So, for example, if a records system is populated with information about a number of individuals, the simplest way for it to function is to permit any authorised user to have access to any and all records, thereby giving the user the maximum functionality and allowing them to do whatever they may wish with the stored information. In many systems the embedded functionality is all-important, since

the data that is being collected is normally made available (for a fee) to commercial operators who use it to generate business opportunities, thereby improving the financial viability of the system and maximising the income from it. Examples abound of personal information stored in databases being sold to third parties[eg 5,16] without the knowledge of the individuals concerned: the UKs information commissioner has commented that 'the penalties aren't strong enough to stop it'.

The point at issue is that the personal information privacy requirements of a system must be built in to the system from the start: it is often impractical to tack them on after the system is built. The preceding sections outline the parameters which any ethical and legal health information management system must be able to accommodate.

3.1 Confidential Data Disclosures

There is an understandable reluctance to admit to the existence or extent of data losses and the reasons for them, given the potential for legal actions as well as loss of public trust. However the health service appears to be the sector with the largest reported confidential data losses (about 1/3 of total reported incidents[17]), and there is a chronological record of the incidents and how they were perpetrated[14] which provides information as to the events that gave rise to these losses.

Based on the evidence[14] it would seem that the most widely reported acts that lead to confidentiality breaches are:

- Losses
  - through unintended disclosures – eg exposed to the web, sent to the wrong recipient, inadequate access controls etc.
  - through physical loss of paper, media, computers, memory devices, etc.
- Abuses:
  - authorised users abusing their privileges, making improper disclosures, carelessness and fraud
- Hackers and malware:
  - Electronic access by an external (non-authorised) party ('hacker'), including through the use of malware and spyware

However, as outlined above, there are other ways in which personalised data may be abused, some of which go unrecognised and unreported since they are widely seen as part of the 'normal operation' of an institution, even though they constitute clear breaches of the duty of confidentiality to the patient – for example the administrative processing of data with full identifiers attached, and the re-identification during analysis of data that has been previously anonymised.

These have been separated on an empirical basis into 7 distinct problem areas for healthcare institutions (below), and in the following section appropriate strategies for prevention and management of each of these are proposed.

- **Accidental data losses and disclosures** Many personal information disclosures take place because computers or memory devices carrying unencrypted personal health information are lost[eg 18], stolen, sold or discarded. In some instances data is lost in transit; in other instances data is incorrectly sent to the wrong destination[eg19]. Data may also be embedded in hardware that is sent externally for disposal or repair, so disclosing the data unnecessarily[eg 20]. These losses are easily prevented with simple measures.

- **Abuse of access privileges** System users are assigned access rights, but these privileges may enable the user to access records which they are aware they should not: there is a cohort of individuals who will browse the system looking for familiar names, and then accessing confidential data about them for which they have no access rights nor reasons, thereby knowingly abusing their privileges. These is an entire industry based on the lucrative business of persuading such users to look up details to order (eg for employers, insurers, finance houses, attorneys etc) usually with the promise of a reward for information provided - a sad reflection on the business ethics of those receiving this information. Where data is outsourced for processing, responsibility lies with the outsourcing institution, but the data may be abused by the contractors and, unless their abuse is a crime within the jurisdiction where the outsourced processing takes place, it may prove difficult if not impossible to prosecute offenders even if they can be identified.

- **Improper data disclosures** Sensitive personal information may be disclosed by staff of health-related businesses, in some cases because they are not aware of the limits on data disclosures and to whom data may legitimately be disclosed, in other cases because they are deceived into disclosing material that they should not – eg by someone posing as a close relative.

- **Abuse of privacy by information technology staff and contractors** The nature of their work requires that IT staff may have to access files where all manner of confidential information is stored – about patients, staff, user privileges etc. In addition technical staff may have the knowledge and skills necessary to copy, edit, export or delete data, as well as to eliminate traces of their activities, or leave a trail leading to another innocent user. A means has to be implemented to prevent this: this is probably the most difficult problem to resolve satisfactorily.

- **Unauthorised access from outside** There is as always the issue of preventing external hackers from gaining access to systems, but at the same time ensuring that legitimate remote users (eg other clinics, clinicians, patients) are able to access the data/functions for which they have access privileges. Many individuals may be afforded external access privileges, including staff of the enterprise working from home: there is a significant risk where the access routines (usernames, passwords etc) are embedded in computers which may be used by others, or can be stolen, so compromising that secure access.

- **Disclosure of patient identity during routine data processing** As outlined above, the identity of the patient should not appear routinely on screen together with their clinical details when clerks are carrying out their normal daily business and administrative functions of the institution: it is hard to ignore the name of the patient when it is right in front of them – more so if that person is local and happens to be known to them.

- **Re-identification of anonymised and pseudonymised data** It is necessary to address the issue of researchers and analysts who have a range of technical/research database linking and management tools at their disposal which can be used to manipulate the data held for example in major data warehouses in order to retrieve the identity of the patients whose anonymised or pseudonymised records have been made available to them for legitimate research and analytic purposes.

3.2 Practical Preventive Measures

Most of the above can be prevented using relatively simple technical and non-technical measures, along with some minor re-arrangement of the ways in which electronic health information management systems are structured. Importantly education and awareness are a central part of this, together with ensuring that all users are subject to a binding agreement regarding their access rights and privileges. There are some generic guidelines available - for example from the Office of the UK Information Commissioner[21], as well as from the International Standard ISO27001. Below are some specific measures that can be taken specifically in the context of healthcare institutions.

- **Preventing accidental data losses** It seems incredible that large quantities of unencrypted personalised data are permitted to be moved onto portable devices, or exported as files to remote locations. Encryption to render unreadable any data that is to be exported in case it does go astray should be mandatory, and downloads of encrypted data should only be made by and through the IT desk to prevent the encryption step being bypassed. Data should be encrypted asymmetrically: this encrypted data would only be readable by the holder of the private key corresponding to the public key used to encrypt it. Where data is destined for a referring physician (eg about investigations, patient discharge etc) all that should be sent is the advice that the data is ready and where the data has been placed: the legitimate recipient should already have access rights to the patient folder and therefore can access it themselves, whilst an unintended recipient will be unable to read the data. Such communications should in all cases be encrypted.

- **Preventing abuse of access privileges** All users must be aware of and contractually bound by their rights of access and their ethical obligations – but this may not be enough. It is relatively easy to associate a table of authorised users with each patient encounter record. There may be additional temporary users, such as the ward and clinic staff when a patient is receiving inpatient care, and others that may be identified/approved by patient. Patient access authorisations will need a unique mark, with a valid from and to period: this might be provided by a patient health card or other token, plus the PIN. In the event that emergency access to patient records is required and the patient cannot for whatever reason provide this authorisation mark, a one-time access arrangement can be made by a designated duty officer giving a valid reason for the access, and thereby opening an audit trail which should be reviewed and closed with the approval of the patient after the event. All access by individuals

to personalised data should be logged and audit trailed, and these logs reviewed routinely looking for evidence of inappropriate patterns of activity.

- **Preventing Improper Data Disclosures** Education and training of staff regarding information privacy is essential: procedures need to be in place identifying who may disclose patient-related data and under what circumstances. Importantly awareness alone is not sufficient: compliance needs to be actively monitored to ensure improper disclosures are not made.

- **Preventing abuses by IT staff** This is probably the most difficult privacy risk to manage effectively, simply because of the privileges and skills possessed by IT personnel due to the nature of the work. One crucial issue is to ensure that 'back door ports' into the system that can be used remotely by third parties (eg vendors, external technicians) to access files, extract data and change software without direct oversight by internal staff are closed, or at least limited to functions that present no risks to privacy: all such ports should be monitored to detect and terminate unusual activity. The system should be designed such that personalised data in medical records is held within an environment secured by a top level access code: whenever this code is in use, there should be a supervisor monitoring what is done, as well as a data log of the event created that can be examined forensically if needed.

- **Preventing unauthorised external access** This is a problem familiar to all IT service managers – how to keep hackers at bay whilst at the same time not impeding access for legitimate users. Authorised external users must be provided with an access routine that is robust and requires their identity to be authenticated (i.e. not just a username and PIN that can be left in the memory of any machine, and can readily be spoofed). Therefore as well as a robust system-wide personal identification system, every user should have a physical token (eg dongle smart card, fingerprint etc) which can prove they are the authorised user: the reason for such a physical token is that there is only one such in existence, whereas a username can be used by many different people. Communications between external users and the system should, of course, be encrypted to prevent eavesdropping.

- **Preventing disclosure of patient identity during routine data processing** There is no reason why the readily human-recognisable identifiers such as name and address are used in routine data management: all systems assign the patient a system identifier (eg unit record number) which is not readily linked to a name by humans without access to a lookup table: this can serve as well as any other for record identification for internal data management needs. The issue is not one of 'heavy' security, simply of filtering out unnecessary data: there is no difficulty in doing a name lookup if this is required – of course all name lookups by staff should be monitored and audited to ensure there is a legitimate reason for the lookup and to detect unusual patterns of such activity.

- **Preventing re-identification of anonymised and pseudonymised patient data** Data from care encounters is supplied to warehouses, analysts and researchers: provision of personalised data would invite privacy breaches, and therefore it should be anonymised or pseudonymised as outlined above. The use of a random cipher is strong as it makes re-identification difficult: however serial analysis of the data using different parameters makes it mathematically possible to re-identify records if the number of 'hits' from a specific query is sufficiently small. Therefore a process should be implemented which terminates any analysis where the number of 'hits' is too small for privacy to be assured, requiring the analyst to seek specific approval for that enquiry – typically a minimal cell size of around 20 might be selected to support genuine analysis but reject attempts at record re-identification.

  Pseudonymised data, whilst supporting vital longitudinal research, presents a greater privacy risk simply because of the linking of several events over time. Preventing the record for a single individual being extracted is therefore vital, and this can be achieved by removing the capacity to abstract records based on pseudonym. The creative analyst might then address the database directly to find all records tagged with a specific pseudonym: this can also be frustrated by ensuring that the ID attached to records in the database has been re-encrypted at the access layer so that users are unaware of the encrypted pseudonym assigned to an individual. Even so the records may still contain references to family members and contacts in the body text, posing some residual but relatively low level risk.

4 Discussion

Many of the above 'solutions' require no further infrastructure: they could and should be implemented within any information management system. However there are some specifics that merit some further discussion.

Patient Authorisations Information custodians may hold records for patients, but access to personalised patient information should be only with the authorisation of the individual concerned (other than as outlined in the exceptions above). For that to happen patients need to have a means of making those authorisations with a valid from and to date, in a way that can be authenticated and audited. The simplest way of setting this up would be for patients to hold a token (eg healthcare card, insurance card etc) that is issued by a trusted authority and which has been registered/validated for the purposes of health data access authorisations – and possibly also for other instances where verifiable consents may be required (eg consent to procedures etc). The application itself could be added onto any existing card if that is the clients preference, and then used to generate an electronic authorisation (including period of validity if required) for this specific purpose. The application might include the ability to establish a proxy in favour of one or more individuals (eg physicians) to act as their trusted agent(s) in deciding when and how to share/disclose their data to third parties.

As an adjunct to this, each patient record will have a table of those with read access: only those individuals who are identified on the access table will have the right of access. Some individuals may be included on a temporary basis – for example ward staff whilst the patient is an inpatient; other may have automatic access rights – for example those undertaking clinical audits or preparing reports where there is a legal requirement to identify the individual concerned.

Strong Identification It goes almost without saying that users of such an information system need to have a robust means of identifying themselves for connection and use of services, and the system being able to authenticate that they are who they say they are. User login IDs and passwords are probably insufficient, since they can easily be mis-used: users in hospitals have even been known to leave user ID and password combinations stuck to the ward monitor, and routinely use each others logins. For security to work, it is fundamental the system can authenticate each and every user, both locally and remotely. The use of a unique token of some sort seems the only way to achieve this: a device/token that identifies the individual and requires a password to activate it should be the logical choice for this, issued by a regional or national authority. Such a proposal has been put forward by the author elsewhere[22]. The same token can also be used to prepare the users 'normal' desktop on whatever networked workstation they are currently using, to set up their logins to all the services they require ('single sign-on'), and manage their encryption services (see below).

Data Encryption There will be instances where data is passed to a third party electronically on a memory device or as a file transfer. In any such case the data should be strongly encrypted using the public key of the individual receiving the data: the data can then only be read by that individual using their private key. This requires that a public key security infrastructure [16] is implemented across the healthcare service. With data encrypted in this way, losses of devices/media do not pose any significant threat to privacy. This might link in with the previous two sections in the form of a health system token (eg smart card) which can be used to identify robustly and authenticate providers, patients and others in the health sector, to manage patient authorisations and consents and to manage encryption keys. The function of such a device could be extended so that it could keep track of where records for an individual are stored, using a healthcare encounters index with internet 'pointers' to where those records are located – including in a patient-controlled internet-based repository if patients so choose, and as proposed elsewhere[23].

Sharing Data Where proprietary or legacy systems do not readily permit external user access to the requisite functions, data for sharing (eg records of care, test and investigation results etc) can be posted on web servers, and/or uploaded to a patient online data repository. If such data is posted to a web server, it would be encrypted with the public key of the patient: the patient can then use their ID token and private key to access and copy the data as they wish. Those holding a copy of the patient key (ie authorised by the patient to access their records), would also be able to access and download records for the duration of the validity of their key.

Records in data warehouses As outlined above, records in large collections present a real threat to privacy. One approach to this, used in a national health information infrastructure where the author was the designer, is to replace identifiers with an alternate ID: the alternate ID selected was the national healthcare user index number, to ensure that the ID was unique. Records were passed to the national database with this ID attached, but at the access layer to the database the ID was encrypted, so that no-one was aware of the ID attached to the record in the database. Even if researchers were able to get access to the database itself (which would be extremely difficult), searching the database to extract records tagged with a specific patient ID would

produced no 'hits' since all IDs in the database were encrypted. However using the routine analysis tools to access the database permitted all types of analysis of the data, including cross-sectional and longitudinal studies, even though the identities associated with the records were concealed.

5 Conclusion and Summary

Private health information that ought to be kept confidential is often not, even though simple measures could be implemented to secure it better. Seven generic situations where personal information may be disclosed in breach of the ethical principle of personal autonomy and of personal information privacy. Few health information systems are designed with a view to implementing the current applicable legislation requiring both that patients give authorisation for anyone wishing to view their records, and that personal records are made directly accessible to patients. Widespread losses and disclosures of health information run into millions of records annually although this figure could be greatly reduced or even eliminated by taking simple security measures such as encryption. There is a clear need effectively to manage the multiple unique identifiers within the care system, as well as to introduce a system for robust authentication of all involved in healthcare – clinicians, patients, analysts, administrators etc, along with an audit trail of the information which they access.

PKI suggests itself as the logical approach to the encryption of information, and a token of some sort (eg a smart card) seems the most practical way of identifying and authenticating individuals, as well as permitting the patient to exert control over their own data.

The root cause of the current problem appears to be a failure to adopt an appropriate privacy and security conscious mind set when designing and developing such systems, and a failure to implement a monitoring systems to assure that information is being kept appropriately confidential at all times. Once a software system has been developed and installed, it is often almost impossible to retro-engineer appropriate privacy measures into it: they need to be planned and implemented into every level within the design.

5.1 Limitations and Further Research

There are numerous obstacles to research into these sensitive issues. One is that few institutions wish to have made public their shortcomings in the confidential treatment of personal information: they would rather it was kept quiet and behind closed doors: therefore data is hard to obtain. The duty of confidentiality creates a layer of complexity (and potentially cost also) in the handling of patient data that clinicians, administrators and technologists alike would prefer to leave aside in order to get their work done effectively and efficiently. Despite the existence of legislation to protect personal privacy, few patients are aware of their rights, and even fewer feel in a position to exert their rights when they are at their most vulnerable in the care of the doctor. And whilst paying lip service to the privacy issue, few clinics or institutions make any concerted effort to audit that the law or their internal policies on this topic are complied with – unless there is a publicised incident or a complaint. This may change however when the cost of law suits (brought under privacy, data protection or human rights legislation) makes prevention more of a priority.

As electronic records systems become more prevalent, and are being more widely networked and accessed remotely, it is becoming increasingly vital that there should be performance criteria (minimum standards) set down relating to the systems-related functions of protecting personal information privacy. Unless these systems support privacy, there is no real prospect that their users will be able to. Once the functionality is there, it is important that a process of independent monitoring of data logs is implemented to identify where there may be concerns: the monitors would act to ensuring compliance with the law and in the 'best interests' of the patients.

References

1. Civan A, Skeels M, Stolyar A, Pratt W. Personal Health Information Management: Consumers' Perspectives. AMIA Annual Symposium Proceedings. 2006;156–160. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1839450/.

2. Cheng T, Savageau J, Sattler A, DeWitt T. Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students. JAMA. 1993;269(11):1404-1407

3. The Hippocratic Oath. (internet) (cited 23 June 2012). Available from: http://www.nlm.nih.gov/hmd/greek/greek_oath.html

4. Open Security Foundation: Data Loss DB. (internet) (cited 23 June 2012). Available from: http://datalossdb.org/reports

5. Sahadi J. Your Identity ... For Sale. CNN Money: May 9 2005. Available from: http://money.cnn.com/2005/05/09/pf/security_info_profit/

6. Barber G. Electronic Health Records and the End of Anonymity. New Jersey Law Journal 1983 227, October 19 2009. Available from: http://epic.org/privacy/medical/EHRs%2010-19-09.pdf

7. Privacy rights Clearinghouse. Fact sheet 8: Medical records Privacy. (internet) (cited 23 June 2012) January 2011. Available from: http://www.privacyrights.org/fs/fs8-med.htm.

8. New Zealand Government. ICT Directions and Priorities: Trust and public confidence risks. (Internet) (cited 23 June 2012). Available from: http://ict.govt.nz/guidance-and-resources/agency-guides/government-use-offshore-ict-service-providers/trust-and-public-confidence-risks

9. Office of the Australian Information Commissioner. Privacy Act. (internet) (cited 23 June 2012). Available from: http://www.privacy.gov.au/law/act

10. Australian Medical Association (Queensland): Code of Ethics. (Internet) (cited 23 June 2012). Available from: http://www.amaq.com.au/index.php?action=view&view=1275

11. Mercuri J. The Ethics of Electronic Health records. Clinical Correlations 15 January 2010. Available from: http://www.clinicalcorrelations.org/?p=2211

12. Office of the Australian Information Commissioner. National Privacy Principles. (Internet) (Cited 23 June 2012). Available from: http://www.privacy.gov.au/materials/types/infosheets/view/6583#npp2

13. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P 0031 – 0050. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

14. Privacy Rights Clearinghouse – Chronology of Data Breaches 2005-Present (2012). (Internet) (cited 23 June 2012). Available from: http://www.privacyrights.org/data-breach

15. Mole D, Fox C, Napolitano G. Electronic Patient Data Confidentiality Practices Among Surgical Trainees: Ann R Coll Surg Engl. 2006 October; 88(6): 550–553. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1963756/

16. T-mobile staff sold personal data. BBC News 17 Nov 2009. (Internet) (Cited 23 June 2012). Available from: http://news.bbc.co.uk/2/hi/8364421.stm

17. One Third of all Data Security Breaches Occur in Healthcare Industry. SECNAP Network Security (Internet) 2011. (Cited 23 June 2012). Available from: http://www.secnap.com/support/whitepapers/healthcare-security-status-2011.html

18. Memory sticks containing details of more than 600 patients lost by trust. The Guardian, Professional, Guardian Government Computing. (Internet) 13 April 2012 (Cited 23 June 2012). Available from: http://www.guardian.co.uk/government-computing-network/2012/apr/13/healthcare-trust-memory-sticks

19. Evans S. ICO dishes out second NHS data loss fine. Computer Business Review. (Internet) 21 May 2012. (cited 23 June 2012). Available from: http://servicemanagement.cbronline.com/news/ico-dishes-out-second-nhs-data-loss-fine-210512

20. Brighton and Sussex University Hospitals NHS Trust fined over privacy breach. The Independent, (Internet) June 2012. (Cited 23 June 2012). Available from: http://www.independent.co.uk/lifestyle/health-and-families/health-news/brighton-and-sussex-university-hospitals-nhs-trust-fined-over-privacy-breach-7811300.htm

21. Data Protection Good Practice Note – Security of Personal Information. UK Information Commissioners Office, 2007. Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf

22. Neame R, Privacy and Health Information: Health Cards offer a Workable Solution. Informatics in Primary Care. 2008;16(4):263-70. Available from: http://www.ingentaconnect.com/content/rmp/ipc/2008/00000016/00000004/art00003.

23. Brayton J, Finneman A, Turajski N, Wiltsey S. PKI (Public Key Infrastructure). (internet) October 2006. (cited 23 June 2012). Available from: http://searchsecurity.techtarget.com/definition/PKI

Conflicts of Interest

None

Correspondence

Roderick Neame, BA,MA,PhD,MB,BChir,FACHI
University of Queensland, School of Information Technology and Electrical Engineering
16 Glen Eden Court,
Flaxton
QLD 4560
roddyneame@taskcare.com