Keeping your EHR Private: Unique Identifiers need to be used with care.

Dr Roderick Neame and Michael Olson
HIC Ltd, Homestall House, Homestall Lane
Faversham, Kent ME13 8UT, UK

Introduction

Computerisation of healthcare has presented some special challenges that are taking longer than many to resolve satisfactorily. One particular challenge is that of creating the electronic health record (EHR), which is in essence designed to be a patient-centred birth-to-death health passport and record of care encounters. A second challenge is the need to find ways to keep your EHR confidential, yet ensure its' ready availability to those authorised providers responsible for your care.

The basic elements of a personal EHR are records made by providers of care services relating to care encounters. These records are personally identifiable, and therefore must be secured to protect confidentiality. Storing and communicating personally identifiable data creates concerns about preventing unauthorised access whilst still permitting ready access to those who are authorised.

Three general approaches have been proposed to manage this risk: the use of virtual private networks (VPN) for healthcare messages (eg NHSnet); the use of encryption; and the use of record de-identification. Whilst a VPN restricts the users to a predefined group (eg registered medical practitioners) and implements a firewall to keep others out, this alone is inadequate to protect privacy (see following section), and must be supplemented with some other mechanism. Encryption is a powerful means of ensuring that any material accessed without authority remains meaningless without the key: however encryption can be broken if the stakes are high enough; and if encryption is symmetric, the keys may become so widely distributed as to afford little real privacy protection.

The authors viewpoint is that record de-identification is the approach best suited to the needs of the EHR: this concept has been outlined elsewhere [1] and involves removal of all context (patient identifiers, dates, times, places, clinics, providers etc) from the record. However in order to retain the link between the record and the patient, some other identifier may need to be attached – a unique patient identifier. This paper will address some of the issues that arise out of the adoption and use of these concepts.

What does Privacy entail?

In essence 'privacy' is the right of the individual to control who knows what about them. This applies as much to health-related data as to any other personal data. Legally and/or ethically, the requirements of personal privacy are that:

?? information should be collected lawfully and fairly, preferably direct from the patient, for a specified purpose to which the subject has assented and in sufficient quantity only to provide for that specified purpose, should be checked before use

or re-use, and should be destroyed as soon as the purpose(s) for which it was collected are fulfilled

?? information should be stored securely, protected from loss or damage, and from unauthorised access; the subject of the data should know what data is held about them, by whom and for what purposes, and should have access to it, and the right to correct it (or to attach a note where the record cannot be corrected)

?? information may be lawfully used only for the purposes for which it was collected, and may be disclosed only where that is necessary to fulfil those explicit purposes; information may not be used for any other purpose, nor disclosed for any other reason

?? exceptions to the above rules are recognised where the subject gives consent for an exception to be made, or where there is a statute or court order mandating disclosure. Additionally arguments in support of disclosure may be made based on the public interest, the interest of law enforcement, or in order to prevent or lessen a serious threat to public or individual health or safety

In respect of the EHR, these provisions have a number of implications.

First the patient must be able to take control over all movements of their personalised healthcare information – even though a proportion of patients may prefer not to exercise this right. Without the assent of the patient, a provider should not pass a patient record to a colleague (eg a referral), or to an insurer, or to a government agency such as the department of health.

Second the patient must be able to select what information is accessible even to their preferred care providers: there can be no automatic right to access everything about the patient, even though the existence of an EHR would make this practicable. Patients may choose to 'forget' some episodes in their past medical history, just as they often do at present, or to cultivate more than one health 'persona' or identity, associating some episodes of care with one or another but not all their health identities.

Third, a person's entire EHR must be accessible to them to read, and to correct, which must include to delete, edit or amend, where they see fit. Obviously 'tampering' with a care record could have adverse effects on health, but it is a patient's right to control who knows what about them. The implication of this is that there must be two distinct records: one will be kept by the care provider, accessible to no-one else, but available as a medico-legal record of their care; a second copy will be 'owned' by the patient and this can be 'corrected' and disclosed to whomsoever they choose, with the proviso that any tampering should automatically absolve the author from responsibility for the accuracy of the contents.

Fourth, wherever a personalised data set or record is vulnerable to hostile attack (eg in communications), the data must be protected (eg by encryption) or otherwise rendered meaningless to the potential attacker. At the same time there should be no impediment to the ready availability of that record to an authorised user.

Is Privacy Protection Necessary?

There is a division of opinion as to whether it really is worth while investing in privacy protection for medical data: some argue that privacy is a commodity which may be traded off against some other benefit; others argue that it is simply over-rated

in importance. The ethical standpoint is clear: information that passes between doctor and patient is given and received in confidence in the context of providing appropriate healthcare services. Equally clear is that few people, however mundane their health records, welcome seeing them laid bare in public: they do not expect care providers to disclose their health records, just as they do not expect their accountants to publish client financial or tax records.

As far as sharing personalised health data is concerned, the OECD [2] developed guidelines in 1981 based on the ethical management of information, the essence of which is summarised in the dot points of the previous section. More recently the EU drafted (1995) and promulgated (1998) legislation designed to give the force of law to almost all the provisions of the OECD guidelines.

The arguments against a strict privacy regime are in essence that there is a potential for conflict between personal information privacy and:

?? the public interest - eg where individuals in the public eye or holding positions of community trust or public offices misrepresent themselves (eg their mental state)
?? the protection of third parties from harm - for example where a third party may be exposed to harm if information is not divulged
?? the need for law enforcement and public protection - for example where individuals hide behind privacy (eg malpractice) in order to conceal crimes
?? the need for public protection – for example where an individual represents a hazard to the general community (eg a carrier of a serious infectious disease)

Beyond these, there is one final commercial argument – that incorporation of effective privacy provisions into healthcare information management systems may be difficult, perhaps more costly too, and could therefore delay the rolling out of systems.

On the other hand systems that lack adequate security and privacy protection are not trusted by either providers or patients, who may refuse to reveal or record sensitive details, so degrading the value of the system or rendering it useless.

So is it the case that building privacy into EHR developments is necessarily complex, costly or likely to engender delays?

EHR Models

The EHR is comprised of a number of entries, each relating to an encounter with a care provider or therapist – mainstream, complementary or alternative.

In the context of privacy requirements, it must be possible for the patient to determine who should have access to which of their records. To achieve this there seems to be only one practicable way forward – that every record may exist in two copies: one (primary) will always be kept securely by the provider; another (secondary) can be made available for sharing with other care providers, purchasers/insurers etc under the control of the patient. (Of course the patient could delegate this power to control who knows what about their health records to an advisor or relative, but that does not impact the need for this capability to be present.)

The security of the primary record is relatively easy to achieve with normal measures, leaving it accessible to no-one except the author. The secondary (EHR) records must be readily accessible and uniquely linkable with the patient, but that linkage must only be enabled when the patient chooses to permit it and then on an entry-by-entry basis.

Unique Identifiers (UIs)

A Unique Identifier (UI) is nothing more than an alternate name for a person: a UI must be unique to one person, but a person could hold one or more UIs – just like aliases – depending on the 'rules' of the UI issuer.

Considerable development has taken place of healthcare UI systems: almost all healthcare systems formally assign a UI to each patient, principally for the purposes of insurance. This constitutes what we have called elsewhere [3] a 'club': in a normal lifetime each of us joins probably hundreds of 'clubs' – professional associations, legal registers, workplace LANs, facilities (eg libraries) and so on. Each club has its rules and privileges, as well as its ways of identifying its members - UIs - unique club membership or policy identifiers. A patient will have at least one unique insurance identifier (UII), but many will hold more than one – for example relating to national insurance, private insurance, employer-funded insurance, travel insurance etc. For the issue of each UII, the individual is required to enrol and provide a set of data (and usually to make payments).

Users of healthcare services already have many local patient identifiers (LPIs) assigned to them by different providers and organisations (although they are normally unaware of many of these). Problems can arise where one UI is designated for use as a general health sector records identifier, especially where the use of this UI has any function in indexing and/or securing the privacy of the records. Using the UI for indexation means that anyone who knows the UI for a patient can find all their records. Using the UI for security means that these records are open to anyone who has access to the UI-name look-up table. These infringe the provisions of the privacy legislation – that the patient should be in control of who knows what about them on a record-by-record basis.

The real issue here is to explore the basis of the case for formal UI issuance. For insurance purposes there is a clear case – but this may inevitably lead to issuance of multiple UIIs for an individual by each insurer (see above). However linking together care records into an EHR to support continuity and integrity of care across providers does not require a formal process of UI issuance: indeed the risk of linkage by formally issued UI is that it may infringe privacy by enabling too many people to associate one or more records with a named individual. The patient can self-identify from a records perspective, offering a 'health record identity (HRI)' (alternate name) for each encounter, although they may need to present a formally issued health insurance UII for payment purposes.

The patient should be locus of control for all identifiers associated with them, (see figure 1), sharing them only with providers with whom they have a care relationship. As long as patients keep track of their HRIs, they can reassert ownership flexibly as and when they choose. Ownership of an HRI is known only to the patient and those care providers that he/she has shared it with. Where an episode of care is to be kept 'secret', it can be assigned an HRI which is unknown to anyone excepting the patient and the provider(s) concerned in that episode.

In this way a basis for developing and managing EHRs in a confidential way can be established. Each EHR (secondary) care record is linked to the patient concerned through one or other of their HRIs: each HRI is known only to the immediate providers of care associated with that episode of illness. Therefore using HRIs as the primary key for linkage of EHR record elements fulfils all the requirements of the privacy legislation, as well as the ethical and social expectations of the community.

Further, removal of all other personal identifiers (name, address, date of birth, encounter date, time and place, etc) renders the record unidentifiable to anyone except those knowing the various HRIs, and makes it possible to store and communicate these records in total security even across open unsecured networks.

Whilst this may at first glance seem a complicated arrangement (see figure 1), in practice it need not be so. Many patients will likely adopt just one HRI, and therefore permit all their records to be accessible to all their care providers, but, crucially, to no-one else. But some patients may prefer to keep one or more aspects of their healthcare separated from the others, for example treatment for cancer or HIV or depression, and they will adopt additional HRIs as necessary.

A mechanism for holding securely these identifiers is required enabling the patient to reveal as many of their HRIs and other identifiers to care providers, advisors, relatives and others as they wish. This could be held locally by the patient (eg using a smart card) or held in a file somewhere in cyberspace but accessible only by the patient.

Conclusion

The arguments that privacy is not really important and that privacy protection is too difficult or costly are specious. The real argument is whether we can afford to proceed towards the EPR without having properly addressed the issue of personal privacy protection. Experience shows that inadequate attention to privacy protection has become a show-stopper in terms of rolling out information systems.

At the heart of this issue is how individuals are to be identified. An individual needs a UI for each 'club' in order to access the benefits of membership. Already individuals are assigned numerous UIs by healthcare providers and agencies. The case for formal identification for insurance (UII) is clear. However the case for a formally issued UPI for sharing of medical records and to underpin the EHR development is not made. Whilst it remains an option, it also opens the door to abuses by anyone who has access to the identifier-name look-up tables, and it need not act to empower patients to control access to their records.

The patient should be able to take control of their identities, and to self-identify (using an HRI) in any appropriate way as far as their personal health records are concerned. That is the essence of the scheme that is proposed in this paper.

Contact Information

Dr Roddy Neame, MA, PhD, MB, BChir
Mr Mike Olson, DipBusStud, DipBusAdmin, MBS
Directors, Health Information Consulting Ltd
Homestall House, Homestall Lane, Faversham, Kent ME13 8UT
Tel: 01795 537896; Fax: 01795 538390
Email: hic@health-info.co.uk; URL www.health-info.co.uk

References

1. Neame RLB (1999) Using the Internet to enable a patient-centred EHR Proceedings of Toward an Electronic Health Record Europe TEHRE'99; Newton, Mass: Medical records Institute, 198-203
2. Guidelines on the Protection of Privacy and Trans-border flows of Personal Data. Paris:OECD 1981

3. Neame RLB and Olson MJ (1999). Strong Authentication of Identity – an urgent issue. Proceedings of Toward an Electronic Health Record Europe TEHRE'99; Newton, Mass: Medical records Institute, 406-410

Figure 1 – a diagrammatic representation of the association between Unique Identifiers and the EHR. The patient controls the secondary records of their own care within the dotted line box, and the links between UIs and HRIs. The provider continues to own and keep confidential the primary record of care, and can update the secondary record as new information comes to hand