Communications and EHR: Authenticating Who's Who is Vital

Roderick Neame[1]

Introduction

Increasingly it is becoming essential for individuals to be able uniquely to identify themselves and each other, even where they may never meet. Access to and use of privileges of membership, whether of a professional association, credit arrangement, computer service, buyer's club or health insurance policy depends upon the 'members' being able to prove that they are who they say they are, frequently from a remote location.

This infrastructure is essential to the health sector. Patients must be able both to claim their entitlements (eg insurance) and assemble their confidential medical records wherever they are. Providers must be able to access secured services and assert their privileges (eg issue prescriptions) from wherever they are. Institutions must be able to recognise both patients and providers and accord them their due rights and privileges.

To do this proof positive of who's who is essential. Two linked problems stand in the way of progress. Individuals need to be able to identify themselves quickly and easily as 'club' members, often from a distance: this could be addressed by establishing sector-wide unique identifier (UI) systems. However such national/centralised UI systems alone are not a solution: in fact they may add to the security problems. UI systems facilitate linkage and retrieval of records relating to a specific individual (identified by their UI), perhaps without their consent, and enable anyone with access to the UI look-up table to identify who that individual is.

This paper proposes a mechanism to deal with these issues.

Setting the scene

1. The patient perspective

Patients should expect that any doctor can provide them with appropriate care. For example if they become ill or suffer an exacerbation of an existing condition at home or whilst on holiday, or are involved in an accident, or attend a clinic where they have not been before, they should be able to expect that their care will be appropriately informed by current and past care events. There should be an overall integrity and continuity in the delivery of care services. At the same time patients may be sensitive and secretive about certain parts of their record, which they may wish to keep confidential from all other parties.

The patient should be able to access and read their own records of care, both in order to understand their problems, the issues that confront them and the choices open to

[1] Dr Roderick Neame, MA,PhD,MB,BChir is managing director of Health Information Consulting Ltd, Homestall House, Homestall Lane, Faversham, Kent ME13 8UT, UK.
Contacts: fax:+44 1795 538390; www.health-info.co.uk; roddy@health-info.co.uk

them, to play a more active role in their own care, and to be able to seek advice from information resources, human or computerised.

Patients expect to be able to make use of their entitlements to care services purchased on their behalf (eg through insurance). They expect that invoices will be passed automatically to the respective purchaser(s) after the patient has accepted and authenticated them as an accurate summary of the care provided.

The professional perspective

Professionals need access to secured computer systems and services in order to discharge their professional duties. A professional may have one or more provider identities (PI) – for example one PI as a GP and another as a part-time hospital registrar or casualty officer. Each of these formal identities will be issued by a trusted authority: each will confer functional privileges (eg to issue orders for medications) and permit access to secured services – computing network, pathology results etc.

The accumulation of userIDs, passwords, encryption keys and so on necessary to establish those secured connections in an increasingly extensive and networked environment is fast becoming too complex for an individual to remember and manage. What the health professional needs is a mechanism to authenticate their PIs and to establish their privileges and secured information systems access rights with the minimum of effort – but complete security.

Issuing and Assuming Identities

In both the above situations, the principle is the same. Patients and professionals must be able to authenticate that they are who they say, and that they own one (or more) 'identity' which is associated with various records and/or privileges.

Issuing an identity may be simple or more complicated, depending upon what privileges are conferred by that identity, and therefore what levels of proof may be required to support that identity. For example a license to practice confers extensive rights and privileges: to obtain a practising identity, a doctor must be able to demonstrate that they meet legal and health agency requirements (usually a qualification and entry into a register). By contrast there is no formal requirement to prove status as a patient: an individual should be free simply to assume an identity of their choosing. However to benefit from health insurance that individual will need an insurance identity formally issued by their insurer: enrolment in an insurance scheme may entail a level of proof, including provision of data and its authentication, as determined by the insurer. Once an identity has been issued, the holder merely needs to be able to authenticate that they are the person to whom the identity in question was issued.

One approach to this involves every individual being vouched for by a trusted third party, to whom they would prove their identity in order to acquire a single 'cyber-identity' – a national identifier. Such an approach has been widely advocated and has been implemented as an identity card in some jurisdictions – notably those with more totalitarian regimes. However this is strongly opposed by civil liberties groups, and not without good reason. Whilst the concept is elegant and well serves the needs of administration, it may be viewed as a serious threat to civil liberty and to the right of an individual to control who knows what about them – a cornerstone of information privacy and human rights provisions. It is a short step from having a national unique identifier to using that to carrying out cross-sectoral data trawling and matching expeditions, which is generally considered ethically unjustifiable unless there is *prima*

facie a basis for suspicion of illegality. Individuals must be free to assume an alias and to partition their information and identity as best suits their needs, except where it is done to conceal a crime or to escape detection.

In summary this section argues that:

1. There are many 'clubs' to which people may belong. Each club assigns an identity to each individual, and may require a level of proof of identity and entitlement to join the club, as well as a consideration (usually money).
2. Each person should be free to hold as many identities as they choose, subject to any requirements of the clubs to which these identities pertain. They can link themselves with any/all of the identities issued to them whenever they wish in order to gain the benefits of 'club' membership
3. None of the above precludes the issuing of a national/international unique identifier, which has the appeal of administrative convenience. However where that unique identifier can be applied across sectors, and where the holder has no control over access to data linked with that identifier, potentially significant privacy issues and infringements may easily arise.
4. There is no reason to restrict the creation of patient identities – although where individuals wish for the services they consume to be paid for by an insurer they will need to prove that entitlement and identity through a formally issued insurance identity.

Towards Patient-centric Records and the EHR

EHR developments must ensure that confidential patient information is available to support the timely provision of best quality care to the patient, whilst keeping their records completely secure. Security is a prime concern: whilst it is argued that having EHR functionality available even at the expense of poor security would be desirable, it is clear that privacy and security are often of over-riding importance to professionals and patients alike, or certainly soon become so once they have been shown to be defective.

Various initiatives have been pursued in order to develop a patient-centric medical record (EHR). Some (eg New Zealand) have established a national health unique identifier and information infrastructure, where key clinical data (such as summaries of significant past care encounters, allergies and sensitivities etc) are recorded centrally and made accessible to authorised users nationwide. Commercial web sites (eg www.drkoop.com) now permit patients to compile their own medical records, and store them: these can be then made accessible by the patient to anyone with a web browser and the access key.

Others have attempted to achieve the same goal but without central records storage, amongst which the UK NHS CareCard[1] development was one of the first. The underlying concept on which this was based was that the entire patient-centric record should be put onto a portable device, carried by the patient and therefore under their direct control. Different devices have been used, most commonly optical or 'chip' cards, but limitations have been recognised in their storage capacity and/or security arrangements, as well as some other dimensions.

Parameters for a Workable EHR solution

There are two ways forward, as illustrated by the above.

1. Either the patient must take physical control over their records entirely, whether hard copy or electronic, keeping them safe and bringing them to future care

encounters, and taking responsibility for all errors, corruptions, losses and so on. Whilst this is possible (and is at present often the only option for those who travel), it seems impractical, inherently risky and will not be explored here further.

2. Alternatively a system must be developed whereby third parties (eg database managers) can store records and make them accessible as and when required by their controller. Links between an individual and their stored records must be capable of overcoming the current confusion of identifiers, where one patient may be known as ABC123 in one place and 456XYZ in another.

We have chosen to explore this latter option. To make it work we need four elements:

(i) Creation of a 'health identity (HI)' (eg Unit Record Number, URN) for the person – this is usually done automatically by every service unit, but the identifier differs from one service unit to the next

(ii) Creation of a link between each encounter record and the relevant personal HI – therefore building common 'threads' to the records

(iii) Establishment of a means whereby a person can assert their ownership of a specific HI and therefore of all records that are linked with it (summarised in a HI-events index), by authenticating that they are the person who 'owns' that HI and index

(iv) Creation of a pointer system that can direct an authorised user to the location where the full record identified in the HI-events index can be found.

Four problems then remain:

(a) ensuring universal readability of the stored records by authorised users;

(b) authenticating the ownership of one (or more) HI by a person;

(c) keeping the stored records secure and free from the risk of unauthorised access or disclosure;

(d) by-passing the security system where a doctor has a duty of care relationship with a patient, but the patient is willing but unable to authenticate their identity (eg forgotten password, lost token etc), or temporarily incapacitated from so doing (eg mental illness, unconscious).

Each of these issues is addressed in the following sections.

(a) Assuring Universal Record Readability

Different applications capture and store records in many forms, but in their simplest form they can be converted to pages (electronic or paper) of text or images. These can be shared using world wide web (www) servers, browsers and basic mark-up language (html). Value can be added through the use of mark-up language extensions (eg XML) or document type definitions (DTD) to structure the contents.

(b) Authentication of Identity and Proof of Ownership

The key to identification and authentication is to hold something that is unique, cannot be duplicated, is easily read by a computer but whose electronic 'signature' cannot be copied or emulated by another device. Various options exist, but our preference has been towards chip ('smart') cards: correctly configured these tokens are easily readable by computers, but difficult to copy, or read without proper authorisation.

The link between person and token must be authenticated, usually by a personal identification number (PIN), but this can be augmented with a biometric identifier (eg

digital photograph, fingerprint or iris scan). The PIN or a digitised copy of fingerprint or iris scan can be held in a secret area on a personal chip card for direct comparison. The presence of the genuine token must also be proven, particularly where the parties are remote from each other, and this is a special advantage of the chip card. To prove that the card is not being emulated, a challenge can be sent based on something that only card and challenger know or can calculate (eg an algorithm): a valid response confirms the token is present.

(c) Privacy and Security of Records

Electronic datastores and communications are always at risk of unauthorised access. Various technical countermeasures can be implemented, but most can be broken by determined (or lucky) hackers, some with only a modest investment of time and effort and a sophisticated toolkit. The key to secure data storage and transfer is to render the data truly meaningless except to the intended user.

We have approached this as follows. When an encounter takes place, one product is a (primary) record of care: this remains where it is created by the doctor concerned and constitutes the medico-legal record. The primary record can be used to generate a secondary copy, edited specifically for the purposes of sharing: the secondary copy comprises only content (complaint, diagnosis, medications, tests etc) and lacks any reference to context (date/time/place, provider, institution, patient, addresses etc). This transform renders the secondary copy meaningless except to someone knowing the context. The context is stored securely under the control of the patient – for example on a chip card – and 'points' to where the secondary copy content is stored (eg on a www server). The card provides any tokens/decryption keys required for record retrieval.

This secondary record store on a www server can be regarded as a patient safety deposit box. Additional copies of some or all of the data from their box could be authorised by the patient and passed to trusted others: these copies could prove beneficial in protecting against the risk of losing the token (see (d) below).

(d) Loss of authentication

If an individual loses their authentication token (eg card), or forgets their PIN, or their token becomes damaged or defective, the default situation is that the patient will be no worse off than now, although the potential benefits of the system may be suspended until the situation can be remedied.

However there are several ways whereby data can be retrieved. For example if the chip card is present but cannot be opened (eg patient unconscious, PIN forgotten) a one-time break-in routine with a 'superkey' has been developed which can be used by an authorised and authenticated doctor to access the device, at the same time writing an audit trail which serves a notification to the owner. Where the card or event index is lost or damaged, the patient may have authorised a trusted third party (eg a doctor) to keep a duplicate copy of the material to guard against this risk, or may have made their own 'back-up' copy. Generally the patient will recall most of their recent care encounters, and could therefore retrieve the most useful data from these providers given a little time and effort.

At another level, the healthcare system within which a patient is normally cared for may reach an arrangement with its members (providers and patients) whereby some data from care encounters are held securely and in escrow against the possibility of such a loss, and can be released under given circumstances. These data would be

linked to a UI (eg insured UI) for the patient. At the same time patients could choose to opt out of this arrangement, recognising that this would incur a risk.

Conclusion

This paper has outlined a mechanism for the secure management of data to support the development of a patient-focused and controlled EHR, potentially accessible anywhere in the world using simple browser technology.

Unique identifiers (UIs) are essential, but may present a threat to personal privacy unless appropriately used. Providers must hold UIs issued by an appropriate registration authority; insured persons must hold UIs issued by their insurer. However patients can self-identify themselves in any way they choose, as long as they have a means of authenticating at a distance that they are the owner of any or all records linked to each of their UIs. There is no need for a one-to-one relationship between patient identity and insured identity: simply that the insurer can be assured that a recipient of care (under whatever identity) is covered by a specified insurance arrangement.

Appropriate records management is crucial for creating a personal EHR with complete security. A secondary record of care is created for each encounter. This can be stored in two ways: either complete in a patient controlled web-based security deposit box; or split into two parts, one part (content without context) stored on any convenient web server, and the other part (including a pointer to the content) held securely by the patient on a personal chip card. In either case, EHR access is achieved through the use of generic browser technology.

Arrangements for accessing the EHR when the patient is unable to provide authentication are outlined, as well as where the UI token (eg chip card) may have been lost or damaged, together with relevant essential safeguards.