Conference papers

Applying new thinking from the linked and emerging fields of digital identity and privacy to information governance in health informatics

John Harrison B Eng MBA
Director, Edentity Ltd, London, UK

Nick Booth MD
Principal Research Associate, Centre for Health Services Research, Newcastle University, Newcastle-upon-Tyne, UK

ABSTRACT

Recent work in the emerging field of network or digital identity suggests a new approach to the design of informatics systems, in which the individual becomes the guardian of their own personal data, and is assisted in controlling access to it by an infrastructure that is aware of roles, such as ‘doctor’, and relationships, such as ‘doctor–patient’. For these purposes, an ‘identity’ is defined as the history of a relationship between two entities, and thus encompasses not only name and address but also data that would usually be regarded as part of an electronic patient or health record. This paper presents a description of how such a true person-centric architecture might work, and shows how it can be seen as an evolution of current plans in the NHS for a national patient data spine. One application, the electronic transmission of prescriptions, is described in detail. Other applications, both within and without the healthcare field, are described in outline. The implementation of such a person-centric system requires a modest degree of technical innovation, but significant change in organisational and business models. It is suggested that there is a need for one or more not-for-profit trusts, each with a remit to act as host for an individual’s digital identity, and as the individual’s true agent. Service providers – such as healthcare organisations – will pay the trust for provision of authentication, and for the storage and transmission of a patient’s data; the trust in turn will pay implementation partners, such as smart card issuers and providers of communication channels, acting on behalf of the individual.

Keywords: digital identity, network identity, person-centric

Introduction

The arrival of near-ubiquitous electronic networks has finally made it practical to realise the goal of true person-centric information technology (IT) systems. The holy grail of health informatics, a true lifelong electronic health record, is becoming a reality. Recognising this, the National Health Service (NHS) has – as part of the ongoing National Programme for IT – drawn up plans for a national repository of personal health data, to be called the national patient data spine. The first (unpublished) specification for the core spine suggests that the design, in the early years at least, will be rudimentary. Patients will be invited to give a one-off consent for use of the spine to store their health data. If consent is given, potentially any NHS professional will be able to gain access to the patient’s data, with professional ethics and the threat of retribution through employment law as the only deterrents to unauthorised browsing. Should the patient refuse consent, data will still be transmitted from local systems to the spine, but will normally only be used in an anonymous form for research purposes.
In the longer term, the NHS envisages that access to a patient’s records will be limited to those professionals who have a ‘legitimate relationship’ with the patient. Leaving aside the difficulties of defining who has, and does not have, such a relationship, the phrase does at least point to one possible evolution path for health informatics systems: that arising from new thinking in the emerging and linked fields of digital identity and privacy. Identity, as we argue below, is all about relationships.

What is identity?

The very word ‘identity’ is unsatisfactory in at least two respects. First, it implies that an individual has a single identity that is used for many different purposes. Although for most people this is close to the truth, one odd effect of the various data protection laws is that, because it is generally illegal for third parties to exchange personal information without consent, an individual could in theory use a different identity for each third party with whom he interacts. As a case in point, note how an individual can be known as ‘J Smith’ to one internet service provider, as ‘Jonathan Smith’ to a second, and as ‘John Smith’ to a third: because the service providers do not—or should not—communicate, there is no reason for the individual to settle upon a single version of his name for all uses. Thus, for the purposes of analysis and system design, it is useful to think about an individual’s many ‘identities’, as shown in Figure 1.

Figure 1 Many identities

Looked at this way, an individual has one or more health identities by which they are known to their various healthcare providers, a fiscal identity for payment of taxation, a legal identity for passport purposes, a private identity by which they are known to a friend, and so on.

The second problem with the word ‘identity’ is that it suggests a defined set of facts about, or attributes of, the individual. In reality, there is no clear definition, and the attributes that go to make up a given identity depend on the purposes for which that identity is to be used. Thus, for voting purposes, the only relevant attributes may be place of residence and age, both of which must be authenticated to some degree: an individual’s legal name is not required, and someone could present himself as Mickey Mouse and still be allowed to vote. For the purposes of an internet chat room, the only necessary attribute is a persistent pseudonym that facilitates recognition from one communication to the next. For building access, the only relevant attribute is whether or not the individual has been given permission to access by the building manager. And for payment systems, the only necessary attributes are a valid account number and knowledge of a personal identification number (PIN). Very few applications require what might be called ‘legal identity’, that is the set of attributes by which an individual is known to the government of a country.

In some circumstances, it is useful to expand the definition of identity to include aspects of the history of the relationship between an individual and a third party. Thus doctors may discuss in the abstract the case of ‘the child diagnosed with Y disease’, using the attribute of the child which for them distinguishes him from any other, and is more memorable than his name. Take this to the extreme, and one can say that identity in its fullest sense is the history of relationships: thus an individual’s medical identities are his various patient records; an individual’s identity at a supermarket is his loyalty account; and a person’s identity with a particular bank includes the frequency with which he goes overdrawn.

Privacy and linkage of identities

One can just about imagine a perfectly private world, in which third parties never exchange information about an individual and every identity relationship is self-contained. But in the real world, with all the pressure to get things done, identities are linked together constantly, sometimes for good reason and sometimes for bad.

Looking at bad practice first, commercial organisations sometimes exchange personal information, and so link identities, without the consent of the individual, and in the near certain knowledge that the individual would not have given consent had he been asked. Such practices are mostly illegal under the
various data protection acts. Examples include the selling of email and street addresses, with spam and junk mail as the unwelcome results.

In contrast, one way of thinking of good practice in data management is as a form of negotiation. Suppose an individual requests an organisation to effect a transaction for his benefit. In response, the organisation informs the individual that certain personal information is required. The individual must then decide whether to comply with the requirement and proceed, or decline and forgo any benefit from the transaction. Examples in the United Kingdom (UK) include the opening of a bank account, where the banks are required by anti-money-laundering legislation to inspect evidence of legal identity; the need to show a birth certificate to obtain a driving licence or passport; and the need — in some difficult cases — to obtain an individual’s consent before information can be shared between health and social care professionals.

But good practice in data management does not always require explicit consent. One example concerns what might be called ‘negative information’, such as a criminal record, where an individual does not benefit from its transmission and so will not give consent. Instead, society has decided that — for the greater good — certain public sector agencies should have access to such negative information, and has legislated accordingly.

Finally, there are many situations where positive information is shared quite legally between different third parties, but where the individual does not give specific permission in a clumsy mechanistic fashion. Instead, access is dictated largely by the role of the third party with respect to the individual: thus a parent automatically has the right to see the school report of a child; a doctor often discusses a patient’s medical history with a colleague, but would never do so with a lay-person; and an individual might look in a friend’s calendar to find out their whereabouts. All of these access rights are conveyed by a combination of role and relationship, and not by explicit consent. Role can be regarded as the pre-qualification for, and relationship as the determinant of, access: an individual might well say that they not only want access to their records to be limited to those with a medical qualification, but — more specifically — to be limited to those who also have a relationship with them, such as doctor–patient, nurse–patient, and so on.

What we lack at present is an IT infrastructure capable of using role and relationship to determine rights of access to personal information, both in the health sector and more generally. In the remainder of this paper, we will outline one possible model — called Virtual Home® (VH) — for such an infrastructure, and then describe early steps towards its realisation.

A new approach to ETP

Suppose, for a moment, that each individual were to be given a point of presence in the network space that could be used to store personal information provided by third parties, either absolutely or in the form of links to data held elsewhere. If such information were to include descriptions of their roles with respect to other individuals and organisations, it could be used to determine access rights to information held in, or accessible through, other points of presence.

This notion conjures up a world of possibilities, in which many such points of presence interact in ways analogous to human interaction in the real world. But immediately there is a naming problem: the term ‘point of presence’ is too cold and impersonal, and since role information can be lifelong, we need a term that conveys permanence as well as trust and security. For now, let us call one of these points of presence a Virtual Home.

To give just one example of its use, think about how someone might obtain, say, repeat medication by post. In many countries this is not currently possible: instead the individual, or their representative, must collect a signed paper prescription from a family doctor, take the prescription to a pharmacist, and then either pay the required fee or sign to claim exemption on any of several grounds. VH allows this transaction to be carried out remotely, and would seem to offer clear benefits over competing designs for the electronic transmission of prescriptions (ETP). The individual gives to their doctor an electronic key permitting write-access to a prescription proforma within their VH. They then give a second key, this time permitting read-access, to the pharmacist who dispenses the required medication for delivery by post, and signs digitally to indicate what has been done.

By requiring the individual to give permission to both doctor and pharmacist in this way, the system observes good privacy practice for the transmission of information. But this is not enough. There is also a need to convince the pharmacist that the prescription is genuine, and it is here that roles begin to be important. Just as in the real world, where an individual must go to a doctor to obtain a prescription but can choose which doctor, so in the network space VH constrains the individual to give write-access for prescription purposes only to a person permitted to exercise the role of doctor. Role information for the pharmacist is also important. Should the individual wish to collect their medication personally rather than have it sent by post, they could give the pharmacist a unique identifier, perhaps carried on a token such as a smart card, and then authorise access by inputting a PIN on a keypad. The VH system will then limit
the pharmacist to seeing only information relevant to their role, and will not disclose any other information that the individual may have chosen to store within their VH. Note, however, that information relevant to the pharmacist’s role may not be limited to that provided by the doctor: the individual could choose also to give them access to information provided by other third parties, such as evidence of entitlement to exemption from payment of prescription charges on grounds of age, chronic illness, low income, prepayment, and so on.

As a slight digression, this prescription application is useful to show how concepts in virtual identity can be extended to apply to businesses, particularly small businesses. If identity is defined as the sum of facts recorded about an entity by a third party, then every transaction results in a modification to the identity of both involved parties. Thus as the pharmacist fulfils a prescription for the individual, and signs on the relevant VH page, they render the individual – or the ‘system’ acting on behalf of the individual – capable of certifying to some third party that a certain kind of prescription has indeed been dispensed, and an appropriate certificate could be stored on the ‘prescriptions dispensed’ page in a virtual pharmacy (VP). This would be useful in situations where pharmacists claim reimbursement from a health insurer for every prescription dispensed: instead of the present cumbersome process of sending bundles of paper prescriptions to a processing centre, the pharmacist would give the reimbursing entity read-access to their VP ‘prescriptions dispensed’ page, whereupon the entity would calculate the amount due by the application of business rules and make payment by bank transfer to the pharmacist’s account, details of which could have been picked up from a different page within the VP.

Other VH applications

Returning now to the main Virtual Home theme, many other applications can be envisaged. Some, like the prescription example given above, involve accounts of different kind: for example, an individual could use their VH to permit sharing of information between a car registration authority and a municipality in order to obtain a parking permit; or to permit sharing of relevant information between medical and social care professionals, probably relying upon the professionals themselves to determine what information is, and is not, relevant for any given transaction. In other applications, the individual could use their VH to establish links between one-to-one records of like kind – such as electronic patient records, bank accounts, exam results and even retail loyalty accounts – so as to create the corresponding one-to-many records, respectively a lifelong electronic health record, a credit record, a validated résumé and a complete retail profile. They could then employ the system of role-based access control to ensure that the information is used only for their benefit. Note that the ability to use VH as a store of a validated résumé fits nicely with the role-based functionality: a doctor could store their medical credentials in their VH, and the system could then use the same credentials in the control of access to medical records.

The common thread that links all of these applications together is the system by which the individual gives consents or permissions. Thus far we have shown how the individual can use this system to exercise control over personal data provided by third parties, but there is every reason to extend its use to cover personal data provided by the individual themselves, such as online calendars, contact books and wish lists. Going yet further, the individual could use VH as the basis for a system of intelligent mail redirection, in which parcels are labelled with a unique identifier rather than a street address, and entities enjoying the role of ‘delivery company’ could use this identifier to obtain a valid delivery address from the VH system – which could be ‘the office’ Monday to Friday and ‘home’ at weekends. And one can imagine a variant of this approach, in which marketing companies pay for a time-limited unique identifier which only maps on to a valid delivery address for a period specified by the individual, thus solving the problems of junk mail and, by extension, of email spam.

Governance and business model

It is quite clear that realising the VH concept requires not only technical innovation, but also significant organisational and commercial innovation. Consider first the nature of the entity that will host a VH: it must be trusted; it must be seen clearly to be on the side of the individual, that is, to act as the individual’s agent; and as a trusted agent it must be financially transparent. These values can only be delivered over the long term by an organisation that adopts objectives consistent with the values. At one extreme, the organisation could be a national government institution, but in many societies few would wish government to act in this role of trusted agent. At the other extreme, the host could also be a conventional commercial company, but again it seems unlikely that people
would wish to entrust a lifelong digital identity to such an entity, especially if there is just one provider rather than a fully competitive market. The right answer is probably a compromise between the two extremes, either a charity or a commercial company with a stated aim of breaking even rather than maximising profit. Initially we might see one of these entities, perhaps called a Virtual Home Trust, for region A, and another for region B, and so on.

A VH trust, as shown in Figure 2, would be governed by a board of trustees, either appointed by another democratic body, or elected using e-voting enabled by the VH system itself. To fulfil its remit as the agent of the individual, the trust would – of necessity – be independent of any token issuer, application provider or communication channel, and would need to develop a system of unique identifiers that was used only to distinguish between different VHSs and was thus one level above the identifiers used by service providers. To maintain privacy, all mappings between service-specific numbers and the individual’s unique VH number would take place within the boundaries of the VH system, and thus the individual’s unique VH number would never be disclosed externally.

In order to make the system viable commercially, the trust would be obliged to act as a clearing house for payments made by application providers (such as municipalities and healthcare providers), and for payments made to implementation partners (such as smart card issuers, mobile network operators and others).

Going one step further, there would seem to be many advantages in requiring the VH trust to keep accounts on a personal basis for each user of the system. Application providers will then pay fees, either on a transaction or periodic basis, as the individual makes use of VH to access their service, and the individual will be able to take their choice, within the limits imposed by technical compatibility, of token issuer and communication channel. The transaction fee approach is not dissimilar to that used by the credit card networks, and will allow the system to grow beyond limitations imposed by a cruder payment method that might seem adequate for any one sector. But there is, of course, one great difference: whereas VISA is a not-for-profit entity that works as the agent of retail banks, a VH trust will be a not-for-profit entity that works as the agent of the individual – and may, although this might appear contradictory, return a profit to individuals who choose to allow use of their data for various marketing purposes.

The idea that VH is completely under the control of the individual raises the question of how many VHSs any one individual might have. In principle, this is for the individual to decide, and only they can make the trade-off between the convenience of using a single VH for many different applications and the risk associated with creating a single point of failure. Note, however, that this risk is mitigated by the fact that frequent use both justifies a higher-quality authentication token and makes it more likely that a user will react quickly to token loss or other security breach. Note also that certain applications, such as e-voting, may require that individuals use a ‘primary VH’, as indicated by the presence of a particular credential, perhaps indicating uniqueness or some other attribute.
Progress to date

As always at the beginning of something new, there is the question of how to get started. Consumer-facing commercial companies are unlikely ever to sponsor the creation of a VH trust because they are jealous of customer data and fearful about intermediation. Departments of national government are little better because, even though they would benefit greatly were VH to exist, they tend to be risk-averse and slow to take up new approaches. In contrast, local and regional administrations are relatively nimble, and are given licence by national government to experiment: there are now signs that something akin to VH may be launched by a consortia of UK local authorities, using funding provided by national government under the various e-government programmes. Whether the NHS can be persuaded to participate remains an open question.

In parallel to this demand-side activity, there are also signs that the supplier base is developing the necessary standards for network identity. One such initiative is the Liberty Alliance, a non-profit grouping set up in 2001 to create open standards in the field;1 and there are competing initiatives from the likes of Novell and Microsoft. But identity management is not primarily a technical problem: substantive progress requires that consumer-facing organisations recognise the need for organisational and commercial innovation, and that takes time.

ACKNOWLEDGEMENT

This paper was delivered at the PHCSG Annual Conference in Cambridge in September 2003.

REFERENCE

1 Liberty Alliance. Liberty Alliance Project Phase 2 Draft Specifications. 2003. www.projectliberty.org

CONFLICTS OF INTEREST

The phrase Virtual Home is a registered trademark of Edentity Ltd. Certain elements of the VH concept are the subject of patent applications.

ADDRESS FOR CORRESPONDENCE

John Harrison
Director, Edentity Ltd
25 Eckstein Road
London SW11 1QE
UK
Tel: + 44 (0)20 7350 1990
Fax: + 44 (0)20 7738 9017
Email: john.harrison@edentity.co.uk

Accepted August 2003