Smartcards

'Smart' Cards - the technology, devices, plans, systems, specifications, business cases...

We have worked extensively with health smartcards, and have a wealth of experience. We can help you seize the opportunities to improve continuity and integrity of healthcare services to consumers, develop integrated patient-centred healthcare records, provide web-based access to key personal emergency data, assure complete privacy of personal information, manage insurance subscriptions, prevent fraud, speed up payments and more.

Why not read and print this overview page, and then
contact us by email today (consulting@hic-ltd.com) outlining your particular interests or concerns - or
- to enquire specifically about our *'Smart Solutions'* overviews.

---

1. What is a 'smart' card?

A smartcard is a plastic card, normally the same size and shape as a credit card, but with one difference. In an internationally standardised (ISO) position on the card there is a set of contacts linked to a computer/memory chip embedded in the plastic of the card - a 'smart' chip. There is no need for physical contacts: the chip can be 'contactless' powered up and accessed by a radio. Of course the card could be made any shape or size. The credit card size and shape has become familiar, and using the same shape allows many existing card features, such as magnetic stripes, holder photographs, embossed characters, signature panels etc to be carried across unchanged for use on smart cards. And of course the smart chips can be embedded in anything, for example in bio-inert capsules for implantation in animals, or as tags on freight to identify the

contents.

'Smart' cards are so called to differentiate them from 'dumb' cards. Dumb cards (eg with a magnetic stripe, optical memory or just a photo) release all their information to any reader without any security. By contrast smart cards are secure: they afford no access to data held on the chip until the chip (1) has been enabled by a password or number, and (2) has checked what data the reader system should be permitted to access. Data can be stored in different areas on the card, each of which can have its own security, and some of which may be designated as inaccessible to all readers (eg security areas). Data stored on the chip is stable (ie no battery is required for the data to remain securely stored).

Back to Top

---

2. Why do we need to use smartcards?

In this section we address four key issues which point us towards the use of smartcards.

2.1 The need for strong authentication of identity

Increasingly it is becoming essential for individuals to be able uniquely to identify themselves and each other, even if they 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.

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

Back to Top

2.2 The need to control 'my things'

Individuals need to be able to prove that an electronic identity and any records stored associated with it belongs to them. That is not to imply that individuals can have one and only one electronic identity – we believe that this is overly judicial and restrictive, unnecessary and contrary to some expectations of civil liberties. But individuals do need to be able to identify themselves in ways that are acceptable to service providers (eg to access a network or restricted web site, to benefit from health insurance, to receive medical care), then to control their 'club membership identities' and to use them to enjoy the privileges of membership as and when they choose. So an individual can have many 'identities' – in fact that is what happens now. You may be known as patient XRD1234 at one health clinic, as NEA0292 at another and as Q/12363/NX by your health insurer (and incidentally as PQ-19832-SR by your tax office). It is your right to keep these separated,

but to prove at any time that you are the 'owner' of any of these identities. The approach we have taken provides for that right.

Hence the role for smartcards. The cards hold the identities and any associated keys (eg passwords, encryption keys etc). The holder controls the card and therefore the identities that he/she owns.

Back to Top

2.3 The need for continuity of patient care

Many patients are in the care of more than one health professional at any time. Then they may go on a short or long visit, or for some reason transfer to other care providers temporarily or permanently. The patient will continue to receive care services: the imperative is to ensure that care services are not to duplicated or omitted and that care plans do not to interfere with each other. For this it is essential that the new health professionals know what the previous ones had done, and know what each other is doing. This minimises waste and risk and maximises potential for speedy, appropriate and effective care.

Back to Top

2.4 The need for integration of stored records

A care provider stores records of care provided to all patients of that service or clinic – if these are electronic we have a conventional electronic patient record (EPR) system. Whilst this may be useful to support care within a particular site, the record that a professional wants to access in order to decide what care is appropriate is that referencing all care services provided to that patient across all care providers – the electronic health record (EHR). The EPR is service-centred; the EHR is patient-centred.

Each record of care is stored in the relevant EPR system with a unique identifier for the patient – unique, at least, to that service. The patient 'owns' that identity (and can prove ownership with their smartcard). To assemble the EHR the patient must assert ownership of all their health identities (or as many as are comfortable), and be able to retrieve the associated stored records. This can be done by storing the records securely and anonymously on web servers, indicating ownership solely through the attached local identifier. The patient card can hold the pointers to these web storage locations and direct a browser to retrieve as many as may be required for the current problem.

Back to Top

---

3. How do we see smart technology being used?

This section essentially summarises the issues that have been raised in the preceding sections, and is therefore brief.

3.1 Smartcards and remote authentication

Individuals are members of 'clubs' and need to be able to assert their membership rights and privileges wherever they may be, more often than not from a remote location across a telecommunications line. Smartcards are ideal for storing identities, passwords, encryption keys and so on associated with asserting ownership and using the privileges of those 'clubs'. The smartcard provides a means of strong authentication as it is unique and secure, and can carry additional on-card security features (eg one-time pad, algorithm etc) to prove the presence of the card and eliminate the possibility of emulation.

Back to Top

3.2 Smartcards and control

The holder of a smartcard is in a position to take control of any functions or data associated with that card and the identities that it holds. So, for example, it can enable a user to activate their privileges on a network, or to access a restricted site on the Internet, or to present a digital certificate of identification from an authority, or to encrypt comunications. It can also permit the holder to record where their data is stored, and assign authority to a third party (eg health professional) to read those records.

We can now move towards ending the present situation where the patient must trust the storing organisation to act in their best interests in determining to whom access to data should be given can be ended. Patients can make those decisions directly, and enact them using them smartcards to provide access to their chosen professionals and advisers.

Back to Top

3.3 On-card security

The card is enabled through a personal identification number (PIN): three incorrect attempts to 'open' the card will lead to it locking and requires a supplier unblocking code to re-activate it. When the card senses a reader attached to it, the two systems check each other in a handshake, and this determines what data, if any, the card will release to the reader.

The card can be configured to carry encryption keys, as well as algorithms. This can permit end-to-end encryption of messages, since they are not decrypted until they reach the card.

The card can also carry a security module. With this the reader system can send a challenge which only that specific card can respond to correctly, thereby confirming that it is present and has not been substituted by emulation software.

Back to Top

3.4 On-card indexes and data storage

The card can be used to store data, although the space available is limited – the most frequently used data is the most useful to store on card. This enables key data to be found quickly, even when network connections may be lost. However data stored on card is not accessible for review or update.

The other essential data stored on the card is an index of where more information is held. Data stored on web-servers, for example, can be maintained and updated by the providers responsible for it, thus ensuring it is fully up to date (eg recent test results). A pointer to the location of these data can be held in the on-card index.

Back to Top

3.5 Using web pointers

The system of web pointers has been developed as outlined above. The location is stored and passed to a browser if that record is to be retrieved. The records themselves, stored in the 'open' on the Internet, are rendered meaningless by either or both of two mechanisms: the context is removed and stored only on the card (with the pointer); and/or the record is encrypted with a key held on the card.

The record stored on the web is only a 'secondary' copy of a 'primary' record held by the care provider. For legal purposes it is the primary copy that must be referenced.

Back to Top

3.6 Further reading...

HIC has various internal documents on this and associated issues. One of these addresses the vexed issue of 'ownership' of health records and how pragmatically to work around this concern. Others address various aspects of system-wide security.

To find out more about 'Smart Solutions' please contact us for further information and advice.

Back to Top