Information in practice

Using the internet to access confidential patient records: a case study

D W Chadwick, P J Crook, A J Young, D M McDowell, T L Dornan, J P New

IS Institute,
University of
Salford, Salford
M5 4WT
DW Chadwick
senior lecturer
A J Young
research fellow

Computer Sciences,
University of
Salford, Salford
M5 4WT
P J Crook
research fellow

Department of
Diabetes and
Endocrinology,
Hope Hospital,
Salford M6 8HD
D M McDowell
principal biochemist
T L Dornan
*consultant
diabetologist*
J P New
*consultant
diabetologist*

Correspondence to:
J P New
john.new@virgin.net

Effective programmes for management of chronic disease are invariably supported by information technology. These have typically been developed within secondary care, with limited access available to primary care. The British government's white paper *The New NHS* clearly states that a dedicated NHS network service (NHSnet), linking information systems in primary and secondary care, will be working by 2002.[1] Although this could improve the flow of information between primary and secondary care, thereby improving patient care,[1] there are, quite rightly, grave concerns about the security and confidentiality of patients' data both in terms of who has legitimate access and who has illegitimate access to the data.[2][3] Furthermore, it cannot be assumed that all general practitioners will be willing to spend the time and money necessary to connect to NHSnet and to conform to its code of connection,[4] especially as more than one in eight general practitioners are already connected to and familiar with the internet[5] and, increasingly, internet service providers are free of charge (apart from telephone charges). Users of NHSnet, however, will be charged for connection and use, the costs of which are not yet known. These are major concerns for general practitioners and may be a reason for the poor uptake of NHSnet by general practice.[5]

In addition, although NHSnet could increase hospitals' and general practices' access to patients' data, this information will still not be available within the patients' homes. This is exactly where general practitioners, seeing sick patients whom they may not know, need immediate access to this information. Internet technology could also allow patients access to their own data, thereby empowering them to allow appropriate healthcare professionals access to their data.

We suggest that the internet will be as good, if not better, an integrating network as NHSnet, providing that the issues of security and reliability can be adequately addressed. Using our existing diabetes information system (Westman Medical Software, Manchester), we have developed a secure, encrypted internet connection that allows general practitioners, diabetes nurse specialists, and, potentially, patients immediate access to the diabetes information system (see figure). We describe the problems, and solutions, that we encountered in ensuring the confidentiality of

> ### Summary points
>
> As an alternative to NHSnet, the internet can be used to access patients' medical records
>
> Patient confidentiality is ensured by using strong encryption and trusted third parties, these are stronger methods than those used within NHSnet
>
> The encryption and strong authentication have been integrated into current browsers (such as Internet Explorer), producing an interface that is familiar to most people
>
> Improved access to patients' data should improve healthcare delivery

the data and in retaining the security of the hospital's private intranet (see table).

Salford diabetes information system

The diabetes information system was introduced in 1992 to facilitate diabetes care within Salford and is used by all local general practitioners and hospital diabetes services. This system is used by 35 districts in Britain, facilitating diabetes care for about 200 000 people. For all patients it contains data, based on the UK diabetes dataset,[6] that are updated and verified during their annual review. The diabetes system prompts these annual reviews in both primary and secondary care. For those patients receiving primary care, the diabetes system generates a single page form containing a summary of the data that is sent through the post to their general practitioner. This system is inflexible; if a patient were to attend his or her general practitioner before the annual review was due this information would be unavailable. Furthermore, after the review the completed form is returned to the central hospital, where the data are entered on to the diabetes system, often several weeks later. An internet connection with the central hospital would allow appropriate healthcare professionals real time access to the diabetes information system.

User authentication

As with all information systems, it is essential that the people accessing the data are who they claim to be. Traditionally, computer systems have asked for passwords to validate users. On a "stand alone" computer or secure private networks (such as NHSnet) this is usually adequate, but not for the internet. The ready availability of "packet sniffers" (programs that sit in a computer network and copy data that are later analysed to extract usernames and passwords) and "cracker programs" (which attempt to find a user's password) make it relatively easy for unauthorised people to obtain passwords. Consequently, passwords that are not encrypted cannot be used for reliable authentication across the internet. We therefore used an encryption technology known as public key encryption (Entrust PKI, Entrust Technologies, Ottawa, Canada) to ensure users were who they claimed to be (table).

Public key cryptography and digital signatures

Asymmetric encryption relies on two keys that work together as a pair—an encryption key and a decryption key. If a user generates a pair of keys and makes the decryption key public but keeps the encryption key private, then only the user can encrypt a message but anyone with the public key may decrypt it and thereby be assured of the sender's real identity (see appendix on the *BMJ* website for further details).

Careful management of public keys is essential. If a hacker successfully substitutes his public key for that of a genuine user he could masquerade as that user and gain access to the hospital diabetes system. The keys are managed by a certification authority, a trusted third party, that validates users and issues digitally signed public keys (certificates) so that recipients can be assured that the owner of the public key is genuine. The Entrust system allows the management and use of public key certificates to be centrally controlled by the trusted third party. Such rigorous authentication procedures ensure that hackers cannot masquerade as a legitimate user.

The security infrastructure

The certification authority server and the public key directory server used to publish all the certificates are housed in a securely fortified room in the University of Salford. Participants have a component of the Entrust software (Direct Client) installed on their computer, which generates the user's pair of keys. It communicates with the servers in order get the user's public key certified, and to download the certified public keys of other users. The certification authority server will issue certificates only to registered participants, so certification is tightly controlled. In addition to the Entrust infrastructure, a user's private key is stored either on the computer's hard disk or on a personal smartcard (Activ-Card Gold, Activcard SA, France). Storing the private key on a smartcard provides increased security, allows users to be authenticated on different machines, and provides for sequential access by many users from the same machine. In order to access the private key a personal identification number (PIN) must be entered, so an
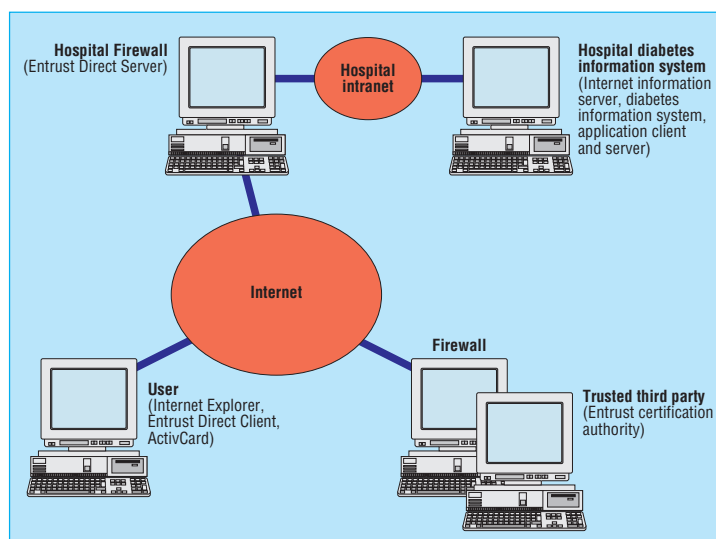
Organisation of internet access to Salford diabetes information system showing location of firewalls, smartcard, encryption software, and trusted third party applications

impostor would need to both steal a user's smartcard and know his or her personal identification number in order to masquerade as the user. This technology and infrastructure enables strong authentication of users accessing the diabetes system over the internet.

Finally, it is essential that healthcare professionals are confident that they are accessing data from the diabetes system and not from a false source. With the same public key infrastructure, a certificate is issued to the diabetes system. Consequently, a user receives a digitally signed message from the diabetes system, providing mutual authentication.

Entry into hospital network

Before a user can be authenticated by the hospital diabetes system, the digitally signed message must be given access to the hospital's private intranet. It is essential to maintain the integrity of the hospital intranet and avoid unauthorised entry via the internet while allowing authorised traffic to gain access. This is a difficult balancing act: too strict a policy will deny authorised people legitimate access to and from the internet, but too lax a policy will allow intruders into the hospital intranet. This

Summary of security problems and their solutions for accessing Salford diabetes information system via the internet

Problem	Description	Solution
User authentication	How does the hospital system know that a remote user's identity is genuine?	Strong user authentication
Establishing access rights	Which parts of the database does a known user have access to?	Access controls on the database
Unauthorised data capture	How do we ensure that no one can take a copy of data being transferred across the internet from the hospital system to a remote user?	Strong encryption of messages
Entry into the hospital network	How do we protect hospital intranet from unwanted traffic entering it while allowing wanted traffic to pass through?	Firewall between the intranet and internet
Easy to use interface	How can we develop a simple yet secure interface that most users will be familiar with and will need minimum training to use and that is low cost?	Web browsers
Correct data source	How can remote users know they have accessed the genuine hospital system and not a site masquerading as the hospital?	Strong authentication of the hospital system

613

security was achieved by installing a firewall (Checkpoint Software Technologies, Israel) between the hospital intranet and the internet and requiring users to be strongly authenticated to the Entrust Direct Server in the firewall. This connection complies with the NHSnet code of connection.[4]

Unauthorised data capture during transmission across the internet

Sending patients' information across the internet, which can be openly accessed and is therefore subject to eavesdropping or interference, requires strong encryption to make it extremely difficult to interpret or interfere with the contents of a message. This was achieved using 128 bit, strong encryption (CAST 128 algorithm) of all the data transmitted across the internet. Any attempt to decrypt such a message by working through every possible key combination would, allowing one attempt every microsecond, take an average of 5.4×10^{24} years (longer than the earth has been in existence). The encryption is automatically initiated after user authentication. This ensures the encryption of all data before they traverse the internet and enables users to access the data unaware of, and not inconvenienced by, background encryption.

Easy to use interface to the diabetes information system

All the healthcare professionals who used the diabetes information system were familiar with the paper version of the diabetes form, and most were familiar with using web browsers (Netscape Navigator (Netscape Communications, California, USA) or Microsoft Internet Explorer (Microsoft, Redmond, USA)). We therefore developed a web based interface to the diabetes system that closely resembled the existing form. The web interface uses hypertext mark-up language (HTML) to present the form to users. The form is generated dynamically from the diabetes server by Microsoft's Internet Information Server. The diabetes server is queried by means of structured query language (SQL), which is generated by computer graphics interface running from the Internet Information Server. Consequently, healthcare professionals can access the diabetes information system in a format similar to the one they are already using via a web interface that they are already familiar with.

To simplify these processes, user verification, encryption, and starting the web browser automatically start after the Entrust Direct Client is launched and the user's smartcard and personal identification number have been inserted. This ensures that all data are encrypted and digitally signed. The Entrust Direct Server then decrypts the message and sends it to the web server, which is oblivious to this intervening security layer. The Entrust Direct Server was located in the hospital firewall system, thereby ensuring that users were authenticated before they accessed the hospital intranet (see table).

Establishing access rights

The existing diabetes system already had simple access controls, with users divided into two groups (general practitioner or consultant) and each group having different privileges to allow them access to their own patients' data. A security table within the diabetes system holds and enforces these privileges.

A simple search facility was incorporated within the web interface to enable users, according to their user privileges, to identify patients and to view and modify their records. All modifications to patients' record are applied in real time, immediately updating the patient records in the diabetes system—a considerable improvement over the current paper based system, where modifications may take weeks before being available on the diabetes system. No data are actually deleted from the diabetes system; mistakes can be deleted from the viewed record but are retained within the diabetes system, being marked "deleted." An audit trail identifies who has made any additions.

Summary

The use of information technology to improve health care is the cornerstone of the government's strategy for the new NHS.[7] We have described a simple to use, yet effective, method for securely connecting a hospital diabetes information system across the internet, thereby providing patient specific information to general practices or even patients' homes. We believe that such systems could be generically applied to most, if not all, forms of chronic disease management. Easy access to clinically relevant information may improve patient care and, by reducing unnecessary duplication of investigations, save money.

Although NHSnet will provide an NHS-wide private network, clinicians should realise that it is not the only solution for providing access to patients' information. We believe that our system is as safe as, if not safer than, NHSnet. The sooner an NHS-wide standardisation for encryption and trusted third party verification is defined the better. Hopefully, these standards will be seamlessly integrated into chronic disease management systems to enable clinicians to fully harness the benefits of improved availability of information without jeopardising patient confidentiality.

1 Keen J. Rethinking NHS networking. *BMJ* 1998;316:1291-3.
2 Department of Health. *Report on the review of patient-identifiable information*. London: Department of Health, 1997. (Caldicott committee report.)
3 Anderson R. NHS-wide networking and patient confidentiality. *BMJ* 1995;311:5-6.
4 NHS Executive Information Management Group. *NHS wide networking*. London: NHS Executive, 1995.
5 Roscoe TJ. Two surveys of internet use in primary care. *He@lth Information Internet* 1998;3:2-3.
6 Vaughan NJ, Home PD. The UK diabetes dataset: a standard for information exchange. Diabetes Audit Working Group of the Research Unit of the Royal College of Physicians. British Diabetic Association. *Diabet Med* 1995;12:717-22.
7 Department of Health. Information for health: an information strategy for the modern NHS 1998-2005. www.imt4nhs.exec.nhs.uk/strategy/index.htm, 1999.

(Accepted 31 May 2000)