How to sign up for a National Care Record Service Acceptable Use Policy: pitfalls and lessons

Mary Hawking
General Practitioner and EMIS National User Group Committee member, Dunstable, UK

Below is an account of problems encountered when trying to sign up for a National Care Record Service (NCRS) Smartcard in the summer of 2005, and the lessons to be drawn from the experience. All opinions are my own.

Introduction

The National Programme for Information Technology (NPfIT) – now National Health Service (NHS) Connecting for Health – was established in 2002 to introduce modern IT into the NHS in England. The three pillars were the NCRS, Electronic Transfer of Prescriptions (ETP) and Electronic Booking (now known as Choose & Book). These functions are carried on the Spine, and access to the Spine is controlled by identifying and authenticating individuals, using a Smartcard, with assigned roles limiting the information seen.

This article is about the process of issuing Smartcards, the form (RA01), terms and conditions (T&C) and NCRS AUP (Acceptable Use Policy) involved, the unexpected problems I encountered and how I tried to address them – with a lot of help from my friends and contacts.

Issuing Smartcards

The NHS is a very large organisation – and access to the Spine will give a large number of NHS staff access to confidential patient information; Smartcards were introduced to prevent access by unauthorised and unidentified individuals.

The process of issuing Smartcards is straightforward. Individuals are sponsored by someone who has known them in the capacity claimed for two years: identity and residence are established by documentation – passport and utility bills; the individual is photographed and a Smartcard containing the photograph issued. This, in conjunction with a password, allows the individual to access Spine functions.

As senior partner of my practice, I was asked to sponsor my partners and practice manager. As far as I knew, this was the extent of my responsibilities; but then I read the form (RA01) which I was asked to sign.

Form RA01 states that by signing, you accept the T&C, and that it is a legally binding agreement. Naturally, I asked to see the T&C (which had not been supplied).

The T&C contained a reference to the NCRS AUP:

10. agree to be bound by the NCRS Acceptable Use Policy (as defined in the Glossary), or as advised by the Registration Authority from time to time and to comply with any changes to the NCRS Acceptable Use Policy notified to me;

The NCRS AUP proved very difficult to find, and when located appeared to be unacceptable for general practice – and unworkable.

A little help from my friends

General practice in the UK has a lot of networks and contacts – and I have been a GP for a long time. As this appeared to be mainly an IT problem, I concentrated on the IT network (my enquiries to the Local Medical Committee [LMC] were met by a certain lack of understanding of the issues involved). I posted my concerns on the Primary Health Care Specialist Group Informatics in Primary Care 2005;13:235–38
(PHCSG) discussion list, and reported to the EMIS NUG Committee. Ewan Davis, Chair of the PHCSG, managed to find the URL for the NCRS AUP. The Chairs of the major GP system supplier user groups and the Chair of the PHCSG sit on the Joint GP IT Committee (JGPITC); the NCRS AUP problem was escalated to the JGPITC, and I am assured, is being addressed.

What was the problem?

Actually, there were several different problems.

Administration of the process

The whole process of signing up for Smartcards appeared poorly organised, and it seems that there was no central direction on establishing NHS Registration Authorities (NHS RA), which NHS organisations were required to set up to issue Smartcards.

Information for Smartcard holders

Why was I not given the T&C at the time I was given the paperwork for sponsoring my practice? If I had not asked for the T&C, I would not have been aware that the AUP even existed. Why was the AUP so hard to locate? After all, the aim of these documents is to make sure that rules are followed – not to take erring individuals to court! Very few of the people asked to sign were given the opportunity to read RA01 before being asked to sign at the time their photos were taken: in at least one case, no signature was required.

RA01, T&C and NCRS AUP

RA01 itself was not a problem. Most of the T&C were not controversial – caring for the Smartcard, observing the NHS Code of Confidentiality, ownership of the card – however, one was impossible: testing the Smartcard as soon as it was received!

11. I sponsored my partners: am I an organisation? Will I be forced to prosecute my partners? And I still don’t know what laws – contract, civil or criminal – apply!

NCRS AUP

There are problems with some definitions and terms used in the AUP.

Authorised Service Recipient means an organisation, including a member of its staff (whether an employee or contractor, and references to ‘staff’ shall be interpreted accordingly), which or who has in either case been duly approved by the Authority and registered by an NHS Registration Authority to use the Service, and includes the following organisations and their staff:

- NHS Registration Authority means an approved individual or team that is responsible for the identification and authenticity of Certificate Applicants, which submits certificates for signing and issuance and for revocation by the NCRS Certification Authority.
- Nominated Security Manager means the Authorised Service Recipient’s representative with responsibility to oversee and ensure the local effectiveness of NCRS security practices, including compliance with this AUP. These responsibilities may include appropriate liaison with Service Provider and Authority staff on relevant IG [information governance] matters and security investigations.

Security in the AUP

Most of the security practices, such as looking after Smartcards and not sharing or writing down passwords, are standard. However, some might cause problems in general practice. In general terms, NCRS security practices include the following (see Table 1), which Authorised Service Recipients are required to observe at all times (acceptable items have been removed).
Table 1 Examples of problems with security requirements in the NCRS AUP (Section 5.8)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring password-protected screensavers are implemented on NCRS workstations</td>
<td>This might cause problems in consultation or other situations where there is not continuous input.</td>
</tr>
<tr>
<td>Not adding unauthorised peripherals such as printers, removable data storage devices or communications adapters to the local NCRS infrastructure, including connections to other untrusted networks</td>
<td>If all systems able to connect to the NCRS are counted as being part of the local NCRS infrastructure, this might make GP systems inoperable; it would certainly create difficulties. GPs use their systems for functions unrelated to the NCRS. ‘Unauthorised software’ implies that some software can be authorised – but no mention by whom or on what criteria. All GPs depend on some third-party software, both for clinical and business purposes. This would prevent developments and innovations, and would be difficult to enforce without total control of every desktop. The modern NHS cannot function without Word and Excel macros.</td>
</tr>
<tr>
<td>Not installing unauthorised software on workstations used for NCRS. Special care shall also be necessary where it is essential to use documents such as Word or Excel that have embedded ‘macros’ to prevent the spread of viruses and the like</td>
<td>I don’t understand this: does it mean that important data may be held locally provided it is backed up?</td>
</tr>
<tr>
<td>Not holding local copies of important data that is not backed up for contingency</td>
<td>A lot of IT equipment in general practice and elsewhere has not been provided by the NHS, and remote access (with proper security) is permitted at present: is this changed because of Smartcards?</td>
</tr>
<tr>
<td>Use only IT equipment that has been provided by the NHS and not, for example, a shared home PC for NHS work</td>
<td>Once you have found out who he/she/it is...</td>
</tr>
<tr>
<td>Ensuring that any identified security weakness, suspected or actual breach of security is reported to the Nominated Security Manager in a timely manner</td>
<td></td>
</tr>
</tbody>
</table>

Apparent lack of consultation

The problems with the AUP have been recognised by NHS Connecting for Health, and the document has been sent to the JGPITC for amendment. To be fair, it was labelled v.1. However, documents of this type are normally distributed to interested parties – including the British Medical Association (BMA) and its General Practice Committee (GPC) – for comment. In this case, this does not appear to have happened, and the reasons for this are not clear. Either the formal channels of communication between NHS Connecting for Health and key stakeholders, including the BMA and GPC, are inadequate or, in this instance, they would appear not to have functioned appropriately. It would be reassuring to know that these channels were being reviewed and improved.

Summary

- Unexpected problems were discovered by one practice trying to sign up for Smartcards.
- Using channels available to anyone in primary care, these were chased, clarified and directed to people able to resolve them.
- There is an apparent lack of awareness of the needs and working patterns of general practice among the authors of the NCRS AUP (and maybe NHS Connecting for Health itself).
- The channels of communication between NHS Connecting for Health and key stakeholders such as the BMA and JGPITC do not appear to have worked in this case.

My final comment: if you find a problem like this, don’t just moan; general practice fields a great team – use them!
NOTES

1 National Programme for IT: established in 2002 to introduce modern IT into the NHS in England. It changed its name to NHS Connecting for Health in 2005.

2 www.npfit.nhs.uk/implementation/documents/ncrsaup_v1.doc

3 There are other key stakeholders, including the Royal College of Nursing and ASSIST: I have no information about whether they were involved.

ADDRESS FOR CORRESPONDENCE

Dr Mary Hawking
Kingsbury Court Surgery
Church Street
Dunstable
LU5 4RS
UK
Tel: +44 (0)1582 663218
Email: mary.hawking@nhs.net

Since this article was written, Philip Brown has been appointed as the Senior Responsible Owner (SRO) for the Registration Authority work, which includes the Registration Authority process and the NCRS AUP.