

How do we connect an optometric practice to NHS IT systems?

Lyndon Taylor
Chairman, AOP Professional Services Committee
December 2007

As enhanced services develop over the next few years, it will become increasingly necessary for optometric practices to transfer confidential patient identifiable data (sometimes referred to as PID) electronically to other parts of the NHS. This will vary from simply sending/receiving reports to direct access to NHS databases or hospital based PAS systems. There is no realistic chance of large scale direct access to NHSNet/N3 for optometric practices in the next few years so this paper attempts to give a brief overview of the options currently available to optometrists.

1) NHSMail

This is a secure e-mail system that allows safe transfer of PID between any e-mail addresses ending in @nhs.net. Note that X@?????.nhs.uk addresses are **NOT** secure. NHSMail is accessible from any internet terminal in the UK via either a web interface or a standard e-mail client e.g. Outlook/Express, Thunderbird etc. These accounts are available via your PCT (or equivalent) and are available to anyone who provides services for the NHS in the UK – this obviously includes optometrists.

Advantages

- No cost to PCT to set up or run
- Easy to use
- Can attach files/documents as per normal e-mail
- Ideal for sending reports or referrals or receiving a specific piece of information e.g. PEARS/referral refinement schemes

Disadvantages

- You are only sending an e-mail to another e-mail address which then requires a person at the other end of the link to read it.
- It is not possible to access a remote database or similar system or to enter data directly into a remote PC. However it is possible to e-mail data files which could then be manually imported into other software.
- One or two PCTS seem to make this route very difficult when it is in fact both free and very easy to implement

Many schemes will find that the no-cost easy option of secure e-mail will provide a simple workable solution in at least the short to medium term.

2) Direct connection to NHSNet/N3

In some ways this seems the ideal solution since in theory it grants access to all necessary NHS services and allows data to be accessed from or entered directly into NHS databases or other systems. However the costs and complexity often make this option impractical.

Advantages

- Direct access to NHS systems
- Ideal for true “co-management” schemes where patients’ care is truly shared between primary and secondary care e.g. co-management of stable glaucoma patients

Disadvantages

- Setting up a direct line to each practice is expensive. Dedicated N3 lines can cost several thousand pounds per annum to run. (Note: there does appear to be a slightly cheaper ADSL-based option available as an alternative)
- The “Code of Connection” issues for these systems are extremely limiting and, in effect, preclude the use of most other software on any PCs so connected.
- It is also not practical in most cases to include an N3 connected PC in a local practice network.
- Almost all installations of this type access the NHS systems through a separate “stand alone” PC which has no connection to other practice IT systems e.g. PCs, network printers or the internet. This is often extremely inconvenient since it requires lots of re-typing of patient info already held on the practice PC system and makes transferring data e.g. images from practice systems to the NHS system positively mediaeval, using disks or possibly memory sticks.
- The need for isolated separate PCs has significant space issues in some consulting rooms and makes access from multiple test/instrument rooms almost impossible.

3) Virtual Private Network (VPN) systems

These offer a (possibly cheaper) alternative to a dedicated N3 line. They come in various formats and allow access via a secure private “tunnel” set up across a normal broadband internet connection. Usually access is limited to a specific service or database. There are two varieties of VPN in use:-

a) Token based

These are usually software based systems and a username is required along with a pass code which is provided by an electronic “token” (a small electronic card which displays the code and changes every minute or two). These are in fairly widespread use by NHS staff for remote/home access to their work servers etc.

Advantages

- Fairly cheap (cost of regular broadband line plus the token itself which is not substantial)

- Often easier to persuade IT departments to endorse than other direct connection options due to easier security setup but at the risk of reduced flexibility for the practice

Disadvantages

- Most token based systems isolate the PC from all other outside contact whilst the VPN is in use. This can be disastrous for many smaller “peer to peer” based practice networks particularly if the consulting room PC is acting as the local server.
- It also makes it impossible to access many other practice systems whilst connected and so once again there is a risk of duplication of effort and difficulties in transferring images etc
- A bit fiddly to log on in some cases
- Security issues in the safekeeping of the token

b) Private Branch Network systems

These in effect make your practice network part of the NHS’s wider network - usually hardware based and managed by a special broadband router. They allow maximum flexibility of working but have security issues which need managing.

Advantages

- All data is available across your local network system, maximum flexibility.
- Used for some diabetic retinopathy screening services to allow images to be taken in a camera room and then graded in a consulting room etc
- Minimum day to day effort in logging on etc
- Fairly cheap to run but routers can be expensive to set up

Disadvantages

- There is a security risk to NHS services.
- A substantial firewall is required at the NHS end of the VPN between the internet/VPN and their systems.
- Usually very limited access only to a very specific NHS service e.g. diabetic retinopathy service, due to security risks above
- NHS IT departments don’t like this approach as it increases the security risk to them and potentially adds a maintenance workload.

END