

# Keeping IT safe: 10 best-practice tips

While it is typically the responsibility of your PCT to manage network and IT security issues, it's down to the practice manager to take care of information security within the surgery itself. In this refresher article, **Alan Hunt** highlights several dangers that you should be aware of, and best practice for overcoming them



**ALAN HUNT**  
CLAS ITPC AlnstISP

**Director of Information Security**  
Hytec

Having spent 28 years in the IT industry, Alan has been involved in many high-profile projects, particularly in the government sector where "joined-up government" provides significant benefits, but is a major information security challenge. Alan is an accredited CLAS consultant (CESG-Listed Adviser Scheme), and is an acknowledged expert in information security policies, ISO 27001 and Codes of Connection. Alan has worked with a number of NHS trusts and currently acts as technical lead on CfH demonstrator and early adopter projects. Alan is married and lives in Rugby – he has a keen interest in aviation and is an avid follower of grand prix racing

For more general practice IT features ...  
[www.managementinpractice.com/IM&T](http://www.managementinpractice.com/IM&T)

It seems that every few weeks there is another story in the press about patient data falling into the wrong hands because of lost USB sticks, stolen computers or network security breaches. The Information Commissioner's Office has shown that it is ready to take action against those who fail to protect patient information, and primary care trusts (PCTs), practice managers and GPs all have a responsibility to keep patient records safe.

There are many steps that you can take at a practice level to prevent data loss and unauthorised access to patient identifiable data. The following 10 points will help you to address some of the most important issues.

## 1. Good Practice Guidelines

Your approach to protecting patient data should start with the Connecting for Health (CfH) *Good Practice Guidelines*, which contain information on risk policies, information governance (IG) policies and training information (see Resource).

It is important to note that:

- CfH updates the Information Governance Toolkit (IGT) regularly; the latest version (v7 – 1 July 2009) contains a number of updates from v6.
- Many managers find the accuracy of their IGT assessment improves after reading the *Good Practice Guidelines*. In fact, it is not possible to provide an accurate assessment without reading the guidance, as the documents in the IG Knowledge Base link to specific requirements that you need to meet.
- You should be ready to provide evidence to support your self-assessment – for example, to show meeting minutes or email communications that prove you have a

particular policy in place. "In place" means approved, published, enforced and regularly reviewed and updated.

- CfH now employs auditors to check that all N3-connected organisations are accurate in their self-assessments.

## 2. Information Governance Toolkit

Practice managers will already be familiar with the IGT provided by CfH. Compliance with the principles outlined in the toolkit is an essential requirement for anyone who wants to access NHS CfH services and the N3 network.

IG is concerned with how you handle patient records, practice information and other sensitive data. GP surgeries need to achieve compliance at level two on the following IG standards:

- IG management.
- Confidentiality.
- Data protection assurance.
- Security assurance.

## 3. Connecting to N3

Once you have demonstrated your compliance with the IGT you will be able to access the N3 network. N3 allows surgeries and other healthcare organisations to share information more easily, and through "community of interest networks" (COINS) you can work more effectively. For example, a hospital will be able to share patients' X-rays with you quickly and easily using a COIN on N3.

There is a common myth that because N3 is a private network it must be secure. Although it is a private network, it is also deemed as "untrusted", which means that you must take extra security measures when connecting to it in order to protect your patient data from outside threats.



In practice, this means that you must follow Cfh guidance, which states that any firewall connecting to N3 must be EAL4-compliant. Your N3 service provider may provide a standard router to help you connect to the network. However, the security features may not offer the necessary protection from external threats. A properly configured, EAL4-compliant firewall is essential in order to prevent unauthorised people from accessing data stored on your surgery network.

#### 4. Mobile and remote working

If you can provide your GPs with secure access to patient information from home and from other locations outside the surgery, you will increase the practice's productivity.

For example, being able to access a patient's notes during a home visit will avoid having to print out the information beforehand and then update the clinical system afterwards. Furthermore, remote access to patient records allows GPs to complete tasks like personal medical attendants (PMA) reports and checking their email, without having to be in the surgery.

To ensure remote access to your IT systems is secure, you must have the following three core technologies in place:

- **Authentication:** checks that a *bona fide* user is attempting to access the network.
- **Encryption:** protects data transferred across the network.
- **Firewall:** protects data at rest on equipment connected to the network.

Even with the technology in place, you will need to ensure that staff take other precautions when remotely accessing patient information. They should not use their home computers because there are no guarantees that the anti-virus protection is adequate, or that the operating system is properly patched and up-to-date. The *Good Practice Guidelines* recommend that only organisation-owned equipment is used. Furthermore, remote workers should not store confidential information on their computer's hard drive unless they have encrypted it using the NHS encryption tool.

#### 5. Role-based access

Your PCT may be able to help you specify a remote access solution, but you should ensure that you can configure it to control user access rights, so that access to patient data matches the role of the person using it. For example, a receptionist may only need to see a patient's contact details and appointment information, while their GP would need full access to the medical history.

#### 6. Allowing others to connect to your network

N3 allows for easier sharing of information between different healthcare organisations, and it also enables your PCT or other third-party organisations to provide remote support for your IT systems. This means that an engineer will be able to fix some issues without having to visit your surgery, and possibly address problems out-of-hours. Furthermore, your PCT will be able to perform routine preventive maintenance – such as anti-virus updates – more efficiently and cost-effectively.

However, you should not allow any third party to access your network without taking the necessary precautions beforehand. You need to ensure that whoever is performing the IT support has a firewall in place appropriate for connecting to N3, which encrypts data and authenticates users. You should also check that your supplier has a relevant, valid and approved IGT and Statement of Compliance (SoC).

The SoC is an agreement between Cfh and approved service providers who are connecting to N3. It sets out the terms and conditions of connecting to the network and ensures that all information will be adequately protected. To obtain approval of the SoC, the supplier has to meet a set of security-related requirements. You can check your suppliers' IGT status by clicking on the "reports" section of the IGT; the status of the SoC can be requested via the Exeter Helpdesk.

#### 7. Safe computing

Computer viruses and other malicious software pose a constant threat to your network. They can

corrupt it, steal it and prevent you from accessing it. To protect your surgery's data from these threats, you must ensure that your security systems – firewall, anti-virus software and operating systems – are up-to-date with the latest versions.

It is also important to highlight these issues to your staff so they are aware of the dangers and can take appropriate precautions. These include not opening attachments from unknown senders, and looking out for "phishing" emails, which attempt to solicit information by impersonating a legitimate organisation.

#### 8. Storing data on devices

Data stored on laptops, portable hard disks, USB sticks, CDs and DVDs can be more vulnerable than desktop PCs because the equipment and media is more easily lost or stolen.

To ensure your data is physically safe there are several simple steps you can take:

- Locking doors within the surgery.
- Securely storing backup media.
- Not carrying removable media such as USB sticks in the same case as your laptop.
- Ensuring that you encrypt patient-identifiable data before storing it.
- Implementing strong controls for data in transit, such as transfer of CDs and DVDs.

#### 9. Caldicott Guardians

Your PCT will have nominated someone to be their Caldicott Guardian. Their role is to provide a focal point for patient confidentiality and information-sharing issues to ensure the management of patient information. The IGT requires that every GP practice has an IG lead, who effectively takes on the local Caldicott responsibility.

It is important that you know the name and contact details of your Caldicott Guardian in case you need advice or further information about your practice's information governance.

#### 10. Further advice

Your PCT can help you identify many of the technology choices that affect information security in your practice, and the head of information management and technology can advise you on how to address these issues. They should also be able to provide you with assurances on the information-security policies, technologies and appropriate controls for the IT services that they provide you with. ■

#### Resources

##### Good Practice Guidelines

[www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/gpgp](http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/gpgp)