



# Joint Guidance on Protecting Electronic Patient Information

## Introduction

There has been much recent media attention around risks to personal data, which is understandable at a time when increasing amounts of data, on many aspects of our lives, are held electronically. Professional, legal and ethical obligations have not changed but everyone in the NHS has a responsibility to understand the implications of dealing with electronic patient data. One of the greatest risks to the security of electronic data is not technology but human behaviour. No data, whether held electronically or on paper, are completely secure. Following best practice guidance, procedures and policies can hugely reduce any risk. This joint guidance is intended to signpost key guidance so that each individual and organisation is aware of their responsibilities in protecting patient information.

## Personal Responsibilities

The General Medical Council (GMC) advises that doctors must be satisfied that there are appropriate security arrangements in place when personal information is stored, sent or received electronically. Personal information is contained in most NHS documents and includes less obvious examples such as patient identifying numbers contained in audit reports. Having an IT team, in your Trust or practice, who can set up firewalls etc does not mean your responsibility ends. A screen can be easily viewed by a passer-by if incorrectly positioned. It is very easy for an 'over helpful' staff member to inappropriately disclose personal information over the phone when it can be brought up on the screen with a couple of keystrokes. It may seem a good idea to share Smartcards as a one off to save time. All these actions jeopardise the security of patient data. Patient data should be treated as securely, if not more so, than your own financial data. You would not, for example, share your credit card with others, leave it in the cash machine or leave your online banking screen logged on. All NHS staff are duty bound to abide by professional and local codes of conduct as well as the NHS Confidentiality Code of Practice as part of their daily working lives. Staff are told to take every care with their Smartcards, and sign up to strict terms and conditions of their use.

Careful consideration should also be given to the use of email. Only NHSmail accounts should be used for exchanging confidential patient information unless it is encrypted. When sending sensitive information precautions should be taken to ensure that those sending and receiving the information know what is to be sent; what it is for and have agreed how the information will be treated. Delivery and read receipts should also be requested so that you can ensure the information has been received safely. Patient identifiable information should not be held on a calendar if it can be viewed by others who are not involved in that patient's care. Further information is available in the NHSmail Acceptable Use Policy (<https://www.nhs.net/AcceptableUse.do>)

If you use a laptop or mobile device you have a duty to ensure that you take appropriate precautions to protect the laptop and the data it contains. This includes reducing risk of theft by keeping the equipment out of sight and locked up whenever possible, using passwords and installing encryption software to protect sensitive data. Your Trust and PCT should have a policy on security for mobile devices and it is your responsibility to ensure that you adhere to this policy. NHS Connecting for Health (NHS CFH) has recently published a laptop security policy which is available at:

<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Exemplar%20Laptop%20Security%20Policy.doc>



If you need to transfer patient identifiable data you have a responsibility to follow the appropriate guidelines. Great care should also be taken with memory sticks ensuring that data is encrypted. Your PCT/Trust should have policies in place and NHS Connecting for Health has recently issued guidance on 'use of encryption to protect person identifiable and sensitive information' described below.

Your Trust or PCT has a duty to ensure that systems are fit for purpose to enable you to carry out your clinical work. If you are unable to meet the requirements of your local security policy because appropriate systems or procedures are not in place then this should be raised. Staff, including medical students, or other students on clinical attachment, should be issued with individual Smartcards. There should not be unreasonable delay when logging onto a system which prevents you from caring for patients. If this is not the case and this is not being addressed by your Trust/PCT please contact the BMA ([info.nhs-it@bma.org.uk](mailto:info.nhs-it@bma.org.uk)) or NHS Connecting for Health ([nhsconfh.communications@nhs.net](mailto:nhsconfh.communications@nhs.net)).

### The NHS Code of Confidentiality

([http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_4069253](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253)) provides detailed guidance on confidentiality issues including a section on electronic data:

- Always log-out of any computer system or application when work on it is finished.
- Do not leave a terminal unattended and logged-in.
- Do not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Do not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pets' names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing of patient information by others.

Good information governance allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively in order to deliver the best possible care. The leaflet 'What should you know about Information Governance' provides further information: <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/infogovleaflet.pdf>.

You should be familiar, understand and question, if necessary, your own organisation's information governance, records management and security policies. You should ensure that you are provided with training so that you are fully aware of your personal responsibilities. You should also be familiar with the NHS Care Record Guarantee and the choices available to patients so that you can support them in their decisions about how they wish their data to be shared (see below).

An audit trail will be kept of every time a patient NHS Care Record is viewed and edited. Staff should only access patient information when strictly necessary i.e. when they, or their immediate team, are directly involved in the care of that patient. Organisations will run regular comparisons of audit trails with the patients who have attended appointments and Caldicott Guardians will receive automated alerts of irregular activity. Patients will be able to request a copy of their audit trail. NHS Connecting for Health and the BMA have supported the Information Commissioner's call for tough penalties for those who unlawfully access patient data.

Documents providing detailed guidance for healthcare professionals about the NHS Care Record Service are available to download at <http://www.nhs-care-records.nhs.uk/nhs/publications> and on the BMA website at [www.bma.org.uk/it](http://www.bma.org.uk/it)



## Organisational Responsibilities

Each organisation should have security, information governance and records management policies in place, which should be endorsed by the Board or senior partners and updated at regular intervals. Organisations must complete the Information Governance Toolkit [www.igt.connectingforhealth.nhs.uk](http://www.igt.connectingforhealth.nhs.uk) which measures progress against a series of standards:

- Information governance management
- Confidentiality and data protection assurance
- Information security assurance
- Clinical information assurance
- Secondary uses assurance
- Corporate information assurance

Each organisation is also required to complete an information governance statement of compliance, which ensures that organisations that use NHS CFH services meet certain standards: <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/background>

Part of the toolkit includes a section on the transfer of batched patient data. Following recent incidents, David Nicholson (NHS Chief Executive) has written to remind chief executives of the protocols for transferring data and further information is available at <https://www.igt.connectingforhealth.nhs.uk/>

David Nicholson has also recently announced that the default position is there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. New guidelines on 'Use of encryption to protect person identifiable and sensitive information' are available at: [https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption %20Guidance%2031.1.2008.doc](https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc). These guidelines detail the recommended encryption standards for when it is necessary to transfer data across the internet or by removable media.

An NHS Information Security Management Code of Practice:

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_074142](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142) is a guide to the methods and required standards of practice in the management of information security. It provides guidance on what should be included in an information security policy.

Records Management: NHS Code of Practice is a guide to the required standards of practice in the management of records. This includes guidance on what should be included in each organisation's records management policy. A records management roadmap provides practical tools and guidance to assist organisations in putting together an effective records management system.

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/records>

The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security and Governance

<http://www.connectingforhealth.nhs.uk/infrasec/gpg>

The Good Practice Guidelines for General Practice Electronic Patient records provides guidance on managing records, information governance issues and security for GP practices

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicy AndGuidance/DH\\_4008657](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4008657)

Organisations must ensure that staff are aware of good practice with regard to security and each staff member should receive regular training including:

- what information they are using, how it should be used and how it should be protectively handled, stored and transferred, including outputs from computer systems;
- what procedures, standards and protocols exist for the sharing of information with relevant others and on a 'need to know' basis;
- how to report a suspected or actual breach of information security within the organisation, to an affected external information service provider or to a partner organisation.



Caldicott Guardians and their support teams will have an increased responsibility and will be responsible for monitoring alerts generated by the NHS Care Records Service. Each organisation has a duty to ensure their Caldicott Guardian and team are properly supported and trained. Further information for Caldicott Guardians including job descriptions and a manual is available at: <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources>

## NHS Connecting for Health's Responsibilities

NHS Connecting for Health is putting the following measures in place to protect patient data:

The IT systems implemented as part of the NHS National Programme for IT have the highest standards of security control and incorporate state-of-the-art safeguards.

**Smartcards** – Access to the NHS Care Records Service will only be possible using a Smartcard and an alpha numeric Passcode, which is known only to the user. The Smartcard is similar to a chip and PIN card. It controls who has access and the level of that access to NHS Connecting for Health systems. The user's name, photograph and unique user identity are held on the Smartcard. In accordance with e-Government Interoperability Framework (eGif) Level 3, Smartcards are only provided when a person has been able to prove their identity 'beyond reasonable doubt' by providing three forms of identity and proof of address to a Registration Authority. To access the NHS Care Records Service, the Smartcard is entered into a reader on the computer and the user must then enter their unique passcode. Even then the user will only be able to see the information they need to carry out their job.

**Legitimate Relationships** – Patient records should only be accessed by those with a legitimate relationship i.e. by the team which is directly involved in that person's care. A patient's registered GP practice would therefore have access although still limited by the access privileges granted at registration. If a patient was referred by the GP to a hospital, a legitimate relationship would be granted to those caring for the patient at the hospital.

**Role-Based Access** – The elements of a record, which can be accessed, will be dependent on the role of the staff member and this is set up on registration. Most staff will be able to access demographic data using their Smartcard. Clinical information can only be viewed if the job role requires access. Therefore a receptionist is likely to see minimal information, such as demographic details and the appointment schedule, whereas doctors would be able to see the full record, although these decisions are taken locally.

**Audit trails and alerts** – Access to the NHS Care Records Service will be audited and alerts will be triggered to highlight possible inappropriate access.

## NHS Responsibilities

The NHS Care Record Guarantee provides a commitment that the patient's records will be used in ways that respect their rights to secure, confidential and accurate records. There are 12 commitments, which include:

- Records will be shared with healthcare teams on a need to know basis
- Identifiable healthcare information will not be shared with other government agencies unless permission has been granted, it is required by law, or approval has been granted for health or research purposes under section 251 of the NHS Act 2006.
- Agreement will be obtained before sharing information with other external organisations such as social services or education.
- Patients can limit how their information is shared.

The full guarantee is available at:

[http://www.connectingforhealth.nhs.uk/nigb/crsguarantee/crs\\_guarantee.pdf](http://www.connectingforhealth.nhs.uk/nigb/crsguarantee/crs_guarantee.pdf)

A new Information Governance Board has been established chaired by Harry Cayton (Chief Executive of Council for Healthcare Regulatory Excellence, former National Director for Patients and the Public and Chair of the Care Records Development Board) to provide advice on information governance in health and social care. The BMA is represented on the board.