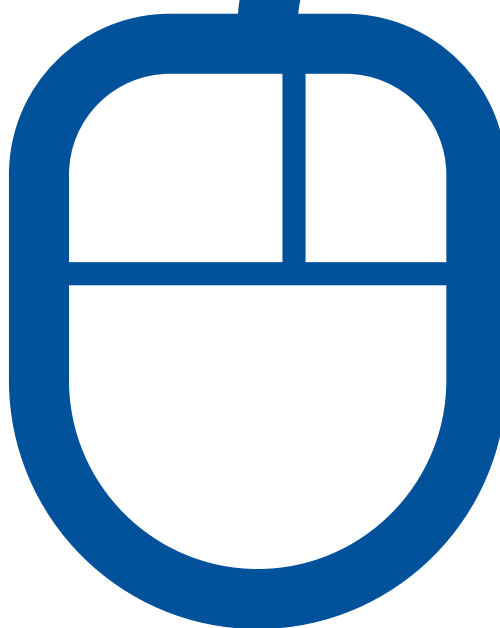
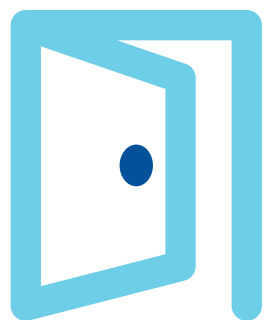


choose and book

# Best practice guidance for information security within Choose and Book

May 2009



# Best practice guidance for information security within Choose and Book

This guidance has been prepared to help organisations understand the importance of information security within the Choose and Book application. It is for organisations who are providing services to NHS patients.

**Patients have a right to expect the NHS to keep their confidential information safe, whether that information is in electronic or paper form. Regulatory bodies have also made it clear that they expect the NHS to put in place the strongest safeguards available to protect patient information. A commitment to achieving this is set out in the NHS Constitution and in the NHS Care Record Guarantee.**

The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the case of the NHS, the most sensitive data is patient record information.

In practice, this is applied through three cornerstones – confidentiality, integrity and availability:

- **Confidentiality** – Information must be secured against unauthorised access.
- **Integrity** – Information must be safeguarded against unauthorised modification.
- **Availability** – Information must be accessible to authorised users at times when they require it.

## Patient information controls

Access to patient information is strictly controlled. There are three main layers of control:

1. **Registration for an NHS CRS Smartcard**  
NHS staff who want to use the Choose and Book application have to register in person with their organisation's Registration Authority. They must prove their identity 'beyond reasonable doubt' and have their access approved by somebody within the organisation where they work. They are then issued with an NHS CRS Smartcard and unique Passcode. They are then issued with an NHS CRS Smartcard and they are asked to set a Passcode only they know. Every time they access patient data, they must use both Smartcard and the Passcode.
2. **Role Based Access Control**  
The information on the Smartcard determines which parts of a patient's information that staff member can access and what they can do (e.g. read only, add information). A clinician may have different access rights to an administration role, for example.
3. **Legitimate relationship with the patient**  
NHS staff will only be able to access a patient's information on the Choose and Book application if they work in a team involved in that patient's care.

As well as access controls, everyone using the Choose and Book application will have their details recorded – who they are and if they viewed, added or changed any information. This 'audit trail' will show any use of the system.

In addition, a 'content sensitive' option is provided so a patient can allow information sharing – but 'seal' certain parts of their information so that those parts are not shared.

**To help minimise the risk of a security breach NHS Connecting for Health has prepared some guidance for organisations. This guidance will help to maintain best practice information security standards when using the Choose and Book application.**

### **Using Smartcards**

If registered Smartcard holders do not keep their Smartcard secure (e.g. share their Smartcard, login details and Passcode with others, or leave their Smartcard logged into a reader when they are not using it), then there is the potential for a third party, to have unauthorised access to confidential patient information, including via the Choose and Book application, under the original user's login details. This might result in a passer-by, having access to patient information without having a legitimate relationship with that patient.

NHS staff must have a legitimate relationship with the patient in order to be authorised to view or access their information on Choose and Book. The Choose and Book application has an audit trail which stores data on the use of the application – allowing appropriate staff to retrieve this data to check that those using the application are authorised to do so. If users do not keep their Smartcard secure or share it with others they could be questioned about inappropriate access, which would be evident on the audit trail under their name.

**Guidance:** All employees have a professional responsibility to ensure that they use their Smartcards, login details and Passcode appropriately. Organisations must stress these responsibilities to their employees when issuing Smartcards and re-enforce them regularly – monitoring Smartcard usage and taking necessary disciplinary action where appropriate.

To remove the risk of unauthorised access in places with many passers-by, organisations also have the option of protecting workstations through screensavers if they wish.

### **Accessing Choose and Book**

Accessing the Choose and Book application, to view a patient's record without the appropriate authorisation, such as for friends, relatives or colleagues, is completely inappropriate.

**Guidance:** Employees should be aware that unauthorised access of the Choose and Book application is not permitted. Organisations have a responsibility to highlight this to employees and provide appropriate training.

### Allocating Smartcard roles

Where an organisation gives an employee incorrect Role Based Access Control to the Choose and Book application, this could allow them to initiate and process referrals on behalf of clinicians, resulting in confidential patient information being viewed and used by employees who do not have an appropriate legitimate relationship with the patient. For example, an organisation gives a non-clinical referral management centre employee incorrect Role Based Access Control to Choose and Book so that they can perform clinical functions, such as processing and initiating referrals on behalf of clinicians. If employees have incorrect Role Based Access Controls then there is also the potential for referrals to be made incorrectly in the Choose and Book application – which could affect patient safety and confidentiality.

**Guidance:** Employees who do not have the appropriate Role Based Access Control and legitimate relationship with a patient should not be authorised to view or use that patient's information. Organisations must ensure they follow the Registration Authority process when allocating Role Based Access Control to employees. The issuing of Smartcards should be overseen by a Caldicott Guardian, who should be fully aware of Role Based Access Controls regulations. Organisations should ensure their process for issuing Smartcards is regularly audited, and take immediate action when any inappropriate use of the Choose and Book application is discovered.

### Printing referral letters

If an NHS employee prints a hard copy of a referral letter for a consultant to review in the 'traditional way', then there is the potential for these referral letters to go astray (as they always could). This could lead to the referral letter being found by a 'third party'. This 'third party' does not have a legitimate relationship with the patient, so they are not authorised to view or access this Choose and Book information. Most 'third party' people would not use the information inappropriately however there is the possibility that the information could fall into the wrong hands.

**Guidance:** The most secure method for reviewing referral letters is online. If providers choose to print referral letters for review, then these letters must not be taken into non-secure areas of the hospital or outside the hospital. Organisations need to ensure that only consultants or other clinicians (e.g. Allied Health Professionals) review these referral letters and that this is done in a secure environment. They should train their employees to adhere to these guidelines. Organisations should also ensure their employees understand that there is the potential for disciplinary action if these guidelines are not followed.

### **Sending referral letters**

If an NHS employee faxes a Choose and Book referral letter to the local Acute Trust, and it is not collected immediately, then there is the potential for confidential patient information to be viewed by other people within the building, including the general public.

**Guidance:** Organisations must take care to ensure that passers-by do not have access to administration areas where printers or fax machines are located. Printers and fax machines should be located in 'safe havens' as dictated by Information Governance policy, and monitored carefully to ensure patient identifiable data is not left in a position where it might be compromised.

It is important to note that the practice of sending of referral letters by fax machine is contrary to optimum use of the Choose and Book application. While this practise is still used for some referrals, such as '2 Week Waits', wherever possible organisations should attach and send referral letters securely via the Choose and Book application.

### **Using NHSmail**

If an NHS employee uses e-mail to correspond with another organisation, then unless both sender and recipient are using NHS Mail accounts then there is the potential for confidential patient information to be viewed by other people within the building, including the general public.

**Guidance:** Organisations must ensure that any e-mail containing patient identifiable data or referral letters is transmitted via NHSmail for both the sender and the recipient. NHSmail provides the ability to securely exchange patient identifiable information between NHSmail users. Government accredited to 'Restricted' status, no other email service available to the NHS has this level of security. NHSmail is also endorsed by the British Medical Association (BMA), Royal College of Nursing (RCN) and Chartered Society of Physiotherapy (CSP) for the purpose of securely exchanging patient data with other NHSmail and GSi users.

It is important to note that item 4.1.8 of the Acceptable Use Policy for NHSmail states that you may only use the NHSmail service for patient referrals if Choose and Book has not yet been implemented in your organisation; the Choose and Book service is unavailable to you for some reason, or the service you need to refer to is not available via Choose and Book.

### Sensitive referrals

Some referrals may be for a condition, treatment or procedure that the patient does not wish anyone else to know about. If an NHS employee does not use the 'content sensitive' functionality in the Choose and Book application for these referrals, then there is the potential for confidential patient correspondence to be viewed by a 'third party' living at the same address as the patient.

**Guidance:** When dealing with sensitive referrals, organisations need to ensure that correspondence is addressed to a place the patient knows is secure. Content sensitive functionality suppresses reminder letters, so depending on the nature of the referral, organisations should consider corresponding with the patient by a different process agreed with them. It is important that organisations ensure that staff managing Choose and Book referrals are properly trained on the 'content sensitive' functionality in the Choose and Book application, and know when it is appropriate to use this functionality.

### Personal Demographics Service

If a referrer is aware of a change in a patient's address or telephone number, but does not update this information in the Personal Demographics Service, then there is the potential for incorrect address or telephone numbers to be used in clinical systems. This could result in confirmation letters being sent to the wrong address or telephone calls made to the wrong number.

**Guidance:** The Choose and Book application sources patient contact details from the Personal Demographics Service, the central source of demographic data. Organisations need to ensure that patient contact details are updated in the Personal Demographics Service. This will help to ensure letters and telephone calls are always directed to the correct place.

### Remote access

If an NHS employee uses the Choose and Book application at home, or another unsecured location, via a Virtual Private Network (VPN) connection to their organisation, then there is the potential for confidential patient information to be viewed by other people within that location, such as friends or relatives.

**Guidance:** Organisations need to restrict use of the Choose and Book application to secure premises wherever possible. Organisations also need to ensure that there is strict guidance for the use of remote access to the Choose and Book application; train their employees to adhere to these guidelines; and take necessary disciplinary action where appropriate.

## Your obligations

Patients have a right to expect that their information is held securely and that their confidentiality is protected.

Privacy and confidentiality require that the Choose and Book application only permits those who have a genuine 'need to know' to access a patient's information – and then only where it is reasonable to believe that the patient concerned would not have objected, if asked for permission.

To support this, NHS Connecting for Health has a range of access controls. These controls provide robust safeguards – whilst also giving patients more control than ever before, over who has access to their information.

Keeping information safe and secure requires the Choose and Book application to meet or exceed national and international security standards. The safeguards in National Programme for IT systems are 'state-of-the-art' and will enable the NHS to meet legal requirements in a way that many older computer systems cannot.

It is essential that every organisation providing NHS services meets its Information Governance Statement of Compliance obligations to the required standards to safeguard NHS services. Data Protection and Human Rights legislation, combined with case law on confidentiality, provide considerable protection for patient information.

The effectiveness of information being held securely and protecting confidentiality in new IT systems depends on the staff who use them. It is important that organisations operate within existing access controls and have appropriate operating policies and procedures in place to ensure a patient's privacy and confidentiality. Where appropriate, organisations should also take disciplinary action where staff have not followed these policies and procedures.