IG Toolkit Version 8

Information Security Assurance

Requirement 322

Detailed Guidance on Secure Transfers
Security Measures for Information Transfers

1. **NHS Encryption Standards**: Guidance on data encryption applications and NHS Information Governance encryption standards is in ‘Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information’ published in December 2008 and is available from the IG Toolkit Knowledgebase Resources.

2. **Digital Transfers over the NHS Infrastructure**: Due to the inbuilt information security functionality (eg NHSmail, Secure File Transfer Service), the NHS infrastructure provides a highly suitable method of transfer of digital information between organisations connected to this infrastructure. Where the use of nationally provided infrastructure services is not possible, information transfer standards and procedures must be agreed and established between organisations to ensure professional, NHS and legal obligations are met. NHS Information Governance guidance is available and will help with these choices.

3. **Encrypted Transfer and Password Protection of Files**: Password protecting files (eg using Microsoft Office) will assist in preventing casual compromise if the file is sent to the wrong recipient but is of little use to prevent a person with a little knowledge or determination accessing the file.

4. **Transfers of Digital Information Stored on Removable Media**: Use of such media for the purpose of storing personal or otherwise sensitive data must be subject to an Information Risk assessment. See Good Practice Guidance ‘Portable Storage’

5. **Transfers of Unencrypted Digital Information by Courier or Post**: On 15 January 2008 the NHS Chief Executive directed the immediate suspension of all transfers by courier or post of unencrypted (digital) data of patient identifiable data (including primary care) unless essential for patient care - and directed that any unencrypted data transfers that continue should be:
a. Signed off by the appropriate organisation’s senior management with a description of how the public will be protected.
b. Notified to the appropriate PCT.
c. Any suspended data transfers to be notified to senior management and the appropriate PCT with a plan for how they are to be replaced or made secure.

6. **Wireless Networks:** There is an emerging use of wireless networks within community pharmacies and dentistry, for example to support connecting laptops in a consultation area to the network without the need for cabling. Expert advice should be sought to set up a wireless network, for example from IT system suppliers. See NHS CFH good practice guidelines on ‘Wireless Local Area Network (WLAN) Technologies’.

7. **Postal / Courier services – general considerations:** The chosen transfer method should be adequately secure and cost effective. It may be acceptable to the organisation to routinely post appointment letters which contain the personal details of one patient but this may not be acceptable for a letter containing sensitive details of a number of identifiable patients.

8. The Drug Tariff (Part II Clause 5) requires that prescriptions being sent to NHS Prescription Services for reimbursement are sent in a secure manner that enables tracking and tracing of the delivery. For other information, it would be for the contractor to decide, based on a risk assessment whether information is sent by post or courier eg based on the volume and sensitivity of information being sent.

9. **Post:** The organisation will need to define the service levels arrangements required from the private or Royal Mail postal service provider:
   a. Secure Post – is a signature required or not required;
   b. Track and trace facility - at individual bag or item level to ensure that items can be identified at any appropriate point in the mail pipeline;
   c. Redirected post – arrangements for;
   d. Undeliverable post - arrangements for.

10. **Courier:** A ‘secure’ courier is not an internal postal service or member of staff visiting a location who may act as a ‘casual courier’. A ‘secure’ courier will provide a secure and tracked mode of collection and delivery rather than a ‘by hand’ / personal delivery service. It will be an organisation providing courier services which provide adequate security assurances set out in a written contract. Some ‘secure’ couriers will allocate a container to an organisation’s items while others may store them in the same container as other organisations’ courier items at lesser cost.

11. For public sector bodies these courier organisations may have already signed up to the ‘OGC buyingsolutions’ framework agreement and therefore already been assessed on the basis of their technical ability and financial standing eg (as at June 2009):
   a. CitySprint
   b. DX Group
   c. E-Courier UK Ltd
   d. Government Car and Despatch Agency
   e. TNT UK
   f. Royal Mail Group

12. There is further information in ‘Secure Courier Procedures’ in the ‘GPG for the transfer of batched person-identifiable data’ available from the Knowledgebase Resources.
13. **Verbal Communications:** The security and confidentiality of telephone and personal conversations should be considered within the organisation’s policy and procedures (e.g., confidentiality code of practice) and included in staff training. Staff should be mindful of the need to maintain security and confidentiality when discussing personal or other sensitive information.

14. **Telephone Answering Machines:** Recorded telephone messages may contain personal or sensitive information such as names and addresses of patients, details of health professionals phoning with queries about patients or applicants for jobs advertised. Consideration should be given to which staff members have access to answering machines. Password protected voicemail boxes can be used to control access where this functionality is available on the phone. Some organisations use a messages book to record messages, care should also be taken to ensure this is stored appropriately.

15. **Internet Protocol (IP) Phones:** IP phone systems allow telephone calls to be made across an internet connection rather than via standard telephony. IP phones are subject to similar security risks to un-secured email, for example ‘eavesdropping’, ‘traffic sniffing’ and ‘unauthorised re-routing’. The level of risk will depend on the size and architecture of the IP phone deployment and pharmacies wishing to implement this technology to transfer personal or sensitive data should seek expert advice from an appropriate information security professional.

16. **Email:** The strategic NHS email system ‘NHSmail’ ([xxx.xxx@nhs.net](mailto:xxx.xxx@nhs.net) addresses) has been designed to ensure the security and confidentiality of NHS information in transit and benefits through the integration of strong encryption technology that automatically encrypts messages in transit. The 2010/11 NHS Operating Framework requires NHS organisations to maximise the benefits of investments already made, to positively impact upon transaction costs. In relation to email specifically, an expectation that NHS organisations and local health communities are expected to take up the quality and efficiency benefits available by moving to full use of NHSmail. (See Key Guidance for a link to the NHSmail website).

17. NHSmail is currently the only NHS approved method for exchanging patient data by email, but only if both sender and recipient use an NHSmail account or if sending to another government secure domain such as:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>GSi (*.gsi.gov.uk)</td>
</tr>
<tr>
<td>b.</td>
<td>GCSX (*.gcsx.gov.uk)</td>
</tr>
<tr>
<td>c.</td>
<td>CJX (*.police.uk or *.pnn.police.uk)</td>
</tr>
<tr>
<td>d.</td>
<td>SCN (*.scn.gov.uk)</td>
</tr>
<tr>
<td>e.</td>
<td>GSE (*.gse.gov.uk)</td>
</tr>
<tr>
<td>f.</td>
<td>CJSM (*.cjsm.net)</td>
</tr>
<tr>
<td>g.</td>
<td>GSX (*.gsx.gov.uk)</td>
</tr>
<tr>
<td>h.</td>
<td>MoD (*.mod.uk)</td>
</tr>
</tbody>
</table>

18. Work is ongoing on the provision of NHSmail accounts for independent contractors and appropriate members of their staff.

19. Other email services should meet NHS encryption requirements. One interim option where NHSmail in not yet used is to transmit patient identifiable information as an encrypted attachment. The NHS recommendation is for AES256 encryption to be employed. This standard is available when using applications such as PGP or WINZIP version 9 or above. With these products the data can be put into a Self Decrypting Archive (SDA) which ensures that it is not necessary for the software that created the archive to be installed on the recipients’ computer. The pass phrase for the archive must be of an appropriate length and complexity and to ensure the safety of data in transit the pass phrase should be communicated to the recipient separately.
from the encrypted data so that the intended recipient is the only one able to decrypt the data. As well as software requirements, consideration would also need to be given to staff training and the workload involved in creating, opening and decrypting an archive. Care would need to be taken to ensure no patient-sensitive information is included in the email itself.

20. When emails including attachments are received containing personal or sensitive information, either via NHSmail or encrypted attachments from other email solutions, they should be stored appropriately on receipt, for example incorporated into the health record and deleted from the email system when no longer needed.

21. Where email is used to send sensitive information, this should be clearly indicated in the subject header, for example marked ‘Confidential’. No person (patient / service user) identifiable information should be contained in the subject heading. See link to ‘Guidance for the Classification Marking of NHS Information’ below.

22. Some companies monitor emails for malicious codes or misuse. Where this is undertaken, organisation email and internet policies should include guidance for staff on what monitoring is being routinely conducted. Comprehensive guidance is available in the ‘Employment Practices Code’ produced by the Information Commissioner’s office and available in the knowledgebase section.

23. **Web Applications:** There are a number of web applications that collect and transfer sensitive or personal information, for example online platforms to support the recording of local enhanced services and internet portals used to collect patient information and requests via the internet. Organisations should satisfy themselves that applications used to support the delivery of NHS services comply with the Confidentiality NHS Code of Practice and have appropriate information security measures in place to prevent unauthorised or unlawful processing or accidental loss, destruction, or damage of personal information.

24. **Remote Desktop Access Software:** There are two circumstances under which it might be necessary to remotely access a desktop computer from a location outside the organisation:

   a. to enable IT supplier remote support - remote access to computer systems is sometimes required by system suppliers in order to provide system support. This will mean that the supplier’s staff will have access to the patient data on the system. This is permissible, as long as the following IG requirements have been observed:
      - any remote access should be used as a last resort, after other actions have been taken (e.g. use of test scripts, diagnostic tools);
      - it must be clear who can initiate & accept the remote logon request - the organisation should retain ownership & control of the actions taking place at that site;
      - the access must be audited - this can be done by the supplier at the support tool level where the Service Desk operative has had to access specific clinical records;
      - the process & policies should be reflected in the IG assurances provided to commissioners and within the IG assurance submission of both the organisation and the system supplier.

   b. to enable use of remote access solutions by staff - there are a number of commercially available remote access solutions that provide an instant secure connection from one PC to another across the internet. For example, this could be used by a contractor with a
wireless internet solution undertaking a service outside the organisation to remotely access records within the organisation.

25. NHS CFH has opted not to approve any remote connection providers but some solutions have been given support by certain PCTs. If using a remote access solution, contractors should satisfy themselves that applications comply with the Confidentiality NHS Code of Practice, seeking expert advice where necessary.

26. **Virtual Private Networks**: Some organisations may wish to create Virtual Private Networks (VPNs) within their business, for example to allow the Head Office secure access to a computer in a particular branch. NHS CFH Good Practice Guidance on, “Site to Site Virtual Private Networks (VPNs)” can be accessed via the Knowledgebase Resources.

27. **SMS Text Messages**: There are various potential applications for text messages in the provision of care services, for example patient reminders to collect prescriptions or attend an appointment. The benefits of using text messages to convey patient information must be weighed against the risks. Key considerations when using text messages are:

   a. is the mobile phone number correct?
   b. is the mobile phone receiving the text message being used by the intended recipient of the message?
   c. has the message been received, and what provision is there to audit message receipt?
   d. text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) - as mobile phones are easy to misplace or may get stolen, there a danger of a breach of confidentiality occurring that the patient may find distressing or damaging.

28. Text messages should not normally be used to convey sensitive information eg test results and the use of text messages for the transfer of personal data should be kept to a minimum, eg an appointment reminder does not need to include the name of a specific clinic.

29. When consent is sought for patient reminder services, patients should be informed of what information will be included in standard SMS messages sent to them via the service.

30. **Electronic Messaging Software**: Electronic instant messaging (IM) software, such as MSN Messenger and Yahoo! Messenger is not suitable for the transmission of personal data as it presents a number of risks:

   a. IM software is particularly vulnerable to malware, such as viruses, Trojans and worms.
   b. In many IM services, data is unencrypted. Such services therefore do not provide sufficient security for transmission of patient data, as they are at risk of unauthorised access and electronic surveillance.
   c. In many IM services, there are no audit trails of access and transmission. The NHS Care Records Guarantee for England has a requirement for systems to maintain audit trails for the access and transmission of patient data.
   d. IM services can be used to bypass restrictions on what can be sent as email attachments.

31. Whilst it is possible that solutions will be developed in future which offer the necessary security and audit controls, there are no IM solutions currently recognised by the NHS nationally as suitable for transmission of personal information.
32. **Faxes**: Fax communications are routinely used, for example, to receive copies of urgently-required prescription forms and discharge communications from secondary care and to support communication with care homes.

33. Faxes containing personal or other sensitive information should be subject to the following NHS IG Safe Haven principles to ensure faxes are safely stored, sent and received and communicated to the recipient:

   a. the sender to phone the recipient to advise them that a fax is about to be sent;
   b. the sender should double-check the fax number and, where possible, use fax numbers that are pre-programmed into the fax machine;
   c. the fax should be sent with a cover sheet stating who it is intended for, and marked “Private & Confidential” to a named recipient;
   d. the sender should ensure the original document is removed from the fax machine;
   e. the recipient should remove the fax from the machine on receipt;
   f. where necessary, the recipient should contact the sender to confirm receipt and that the fax will be appropriately dealt with and safely stored.

34. If the fax machine is being used to receive patient information, it should be sited in a secure location, for example the dispensary or surgery, where access to the machine is controlled.

35. **eFaxes**: eFax software allows users to send or receive a fax via a computer rather than a fax machine. The IG risks for eFax are therefore a combination of the risks linked to email and standard fax communications. There is currently no eFax service recognised as being sufficiently secure to support the routine transfer of patient personal data.

Information Governance Policy
DH Informatics
May 2010