Information Governance Toolkit

Information Security Assurance

Detailed Guidance on Secure Transfers

Information Transfers/Flows - Security Measures

1. The outcomes of information mapping and identified risks should be used to develop staff guidance on appropriate methods of transferring person identifiable and sensitive information in any format (paper, electronic etc).

2. A list of Good Practice Guidance (planned, proposed or already available) to assist secure transfers/flows of information is available from the **Knowledge Base Resources**. The following points should be considered.

3. **NHS Encryption Standards**. See Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information published in December 2008, which contains guidance on data encryption applications and NHS Information Governance encryption standards.

4. **Digital Transfers over the NHS Infrastructure**. Due to the inbuilt information security functionality (e.g. NHSmail, Secure File Transfer Service), the NHS infrastructure provides a highly suitable method of transfer of digital information between NHS organisations and others 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.

5. **Encrypted Transfer and Password Protection of Files**. Password protecting files (e.g. 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.

6. **Transfers of Digital Information (Data) 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 by the Information Asset Owner (or equivalent).

7. **NHS Transfers of Unencrypted Digital Information (Data) By Courier or Post**. On 15th January 2008 the NHS Chief Executive directed the immediate suspension of all transfers by courier or post of unencrypted (digital) data of service user identifiable data (including primary care) unless essential for care, and directed that any unencrypted data transfers that continue should be:

   - signed off by the appropriate organisation's Board with a description of how the public will be protected;
   - notified to the appropriate Strategic Health Authority (SHA);
   - any suspended data transfers to be notified to Boards and the appropriate SHA with a plan for how they are to be replaced or made secure.

8. **Wireless Networks.** See Good Practice Guidance.

9. **Postal / Courier services**. See ‘Secure Courier Procedures’ within ‘GPG for the transfer of batched person-identifiable data’ accessible via the **Knowledge Base Resources**.

10. 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 service user but this may not be acceptable for a letter containing sensitive details of a number of identifiable service users. If the organisation’s procedure is correctly applied and reliable assurance and incident reporting assess that the procedure is adequate, then this will inform reviews of the adequacy of the chosen methods and processes e.g. robust packaging and correct addressing and marking of items.

11. **Post.** The organisation will need to define the service levels arrangements required from the private or Royal Mail postal service provider:

    - **Secure Post** – is a signature required or not required?

    - **Track and trace facility** - is this available at individual bag or item level to ensure that items can be identified at any appropriate point in the mail pipeline?

    - **Redirected post** - what are the arrangements for?

    - **Undeliverable post** - what are the arrangements for?

12. **Courier.** A ‘Secure’ Courier is not an internal postal service or member of staff visiting a location who may act as a ‘casual courier’ (which some organisations refer to as "couriers"). A ‘Secure’ Courier will provide a secure and tracked mode of collection and delivery rather than a ‘by hand’ / personal delivery service. Some ‘Secure’ Courier services 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. A ‘Secure’ Courier will be an organisation providing courier services which provide adequate security assurances set out in a written contract. For public sector bodies these courier organisations may have already signed up to the ‘OGC buying solutions’ framework agreement and therefore already been assessed on the basis of their technical ability and financial standing, eg (as at June 2009):

    - CitySprint
    - DX Group
    - E-Courier UK Ltd
    - Government Car and Despatch Agency
    - TNT UK
    - Royal Mail Group

13. **Verbal Communications.** The security and confidentiality of telephone and personal conversations should be considered within the organisation’s policy and procedures 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 service users, details of health or social care professionals phoning with queries about service users 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. Otherwise, physical protection should be considered, e.g. locating the phone in a lockable office, lowering the speaker volume, etc.

15. **Internet Protocol Phones.** See Good Practice Guidance.

16. **E-Mail - General.** See Good Practice Guidance.

17. **NHSmail.** The strategic NHS email system 'NHSmail' (xxx.xxx@nhs.net addresses) has been designed to ensure the security and confidentiality of NHS information in transit between account holders 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 exists that NHS organisations and local health communities take advantage of the quality and efficiency benefits available by moving to full use of NHSmail. (See the **Knowledge Base Resources** for a link to the NHSmail website).

18. 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:

    - GSi (*.gsi.gov.uk);
    - CJX (*.pnn.police.uk);
    - GSE (*.gse.gov.uk);
    - GSX (*.gsx.gov.uk);
    - GCSX (*.gcsx.gov.uk);
    - SCN (*scn.gov.uk);
    - CJSM (*cjsm.net);
    - MoD (*.mod.uk).

19. NHSmail now includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services. Encryption should primarily be used to exchange sensitive data as part of an agreed clinical workflow, and users should follow any local Information Governance policies that are in place locally for sending sensitive data. All users must be fully trained in the use of email and NHSmail accounts. For further advice on using the NHSmail encryption feature, please see 'HSCIC: Sending an encrypted email from NHSmail to a non-secure email address', available via the **Knowledge Base Resources**.

20. Where email is used to send sensitive information, this should be clearly indicated in the subject header, for example marked 'Confidential'. No service user identifiable information should be contained in the subject heading. See

the **Knowledge Base Resources** to download 'Guidance for the Classification Marking of NHS Information'.

21. **Legal Disclaimers.** The use of disclaimers on websites and correspondence lessen the potential of litigation against staff and the organisation. The use of disclaimers should be considered where appropriate (for internal as well as external correspondence) to address:

    - breaches of confidentiality;
    - virus transmission;
    - contract protection;
    - negligence for incorrect advice;
    - libel and defamation.

22. **Web Applications.** See Good Practice Guidance.

23. **Remote Desktop Access Software.** See Good Practice Guidance.

24. **Virtual Private Networks.** See Good Practice Guidance.

25. **Electronic Diaries.** See Good Practice Guidance.

26. **SMS Text Messages.** There are various potential applications for text messages in the provision of services, e.g. service user appointments. The benefits of using text messages to convey personal information must be weighed against the risks. Key considerations when using text messages are:

    - is the mobile phone number correct?
    - is the mobile phone receiving the text message being used by the intended recipient of the message?
    - has the message been received, and what provision is there to audit message receipt?
    - 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 is a danger of a breach of confidentiality occurring that the patient / service user may find distressing or damaging.

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

28. When consent is sought for appointment reminder services, service users should be informed of what information will be included in standard SMS messages sent to them via the service and the option to opt out must be available on request.

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

    - IM software is particularly vulnerable to malware, such as virus, Trojans and worms;

- in many IM services, data is unencrypted. Such services therefore do not provide sufficient security for transmission of service user data, as they are at risk of unauthorised access and electronic surveillance;
- in many IM services, there are no audit trails of access and transmission. The *Care Record Guarantee* (NHS and Social Care) has a requirement for systems to maintain audit trails for the access and transmission of service user data;
- IM services can be used to bypass restrictions on what can be sent as e-mail attachments.

30. 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.

31. **Faxes and eFax.** Faxes containing personal or other sensitive information should be subject to safe haven principles and procedures (or the equivalent – see Confidentiality and Data Protection requirements) to ensure faxes are safely stored, sent and received and communicated to the recipient. eFax should also be subject to safe haven principles.

32. 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 service user data.