Transferring Patient Identifiable Data
—
Faxing Policy

Introduction ........................................................... 1
Why we need a policy .............................................. 2
Threats and vulnerabilities ....................................... 3
Can I use a fax machine ? ........................................ 4
Access and authorisation ....................................... 7
Transmission procedure ....................................... 7
Audit .................................................................... 8
Facsimile machine settings ..................................... 8
Output handling and sanitisation ............................. 9
Incident reporting ............................................... 9
Annex A - Example of a cover sheet ....................... 11
Annex B – Fax checklist ....................................... 12
**Introduction**

**Background**

In this age of instant communications it has become commonplace to use facsimile equipment to transmit documents; indeed the system is so popular that many private individuals now own their own fax machines.

What many people fail to realise is that faxes have many vulnerabilities which could result in the wrong person reading the sent document. This, of course, bears little weight when the contents of the transmission are not sensitive. If the document contains personal details such as patient identifying details, the duty of confidence each of us have in law dictates that we do not have the right to ignore these vulnerabilities.

**Key messages**

Bearing in mind our legal and moral obligation to protect personal data, the use of fax machines to transmit patient details cannot be condoned. It is, however, clear that in some limited circumstances it is acceptable to use fax machines to transfer identifying details.

The basic tenet when transferring patient identifying data is that in all circumstances where patient identifiable data is disclosed, by whatever method, the data items transferred should be restricted to a minimum. Only those items of data that are essential to the purpose of transferring the data should be included in the document; extraneous and irrelevant items should be omitted or blocked out before transmission.

**The aim of this document**

This document seeks to provide fax users with the background to the threats to security and to lay down guidelines as to when the use of fax may be acceptable and to make the use of fax safer in those circumstances. It has been developed by a community-wide group of Caldicott Guardians with the intention that it be adopted in principle by the organisations represented on the group in order to standardise procedures in the South West area.

**Scope**

This policy is concerned only with the transferring of personal identifying information as defined by the Data Protection Act 1998 and the Caldicott Committee Report, December 1997.

**Caldicott Guardian**

As recommended by the Caldicott Committee, each NHS organisation should have appointed a Caldicott Guardian to take the lead in patient confidentiality issues. Where advice is needed, the Caldicott Guardian should be your point of contact.
Why we need a policy

All NHS Organisations are under a legal, moral and professional obligation to ensure the confidentiality of personal data.

**Data Protection**

The Data Protection Act 1998 requires that:

“appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data.”

The Act also defines processing to include:

“disclosure of the information or data by transmission, dissemination or otherwise making available”

This means that we must implement widely accepted security measures that restrict the transfer and holding of personal data. The Data Protection Commissioner has grave reservations in the security of fax machines for the transfer of patient information.

**Government Recommendations**

The Caldicott Report on the transfer of patient identifiable information, published in December 1997, made sixteen recommendations that are to be implemented by NHS organisations.

The report gives support to the concept of ‘safe havens’, and recommends that the NHS Number should be substituted for patient identifiable data wherever possible and that where patient data is transferred it should be reduced to the minimum required for the purpose.

**Professional Codes**

The General Medical Council’s booklet “Confidentiality”, an associated leaflet to “Good Medical Practice”, stipulates guidance to health professionals. It states clearly:

“When you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is disposed of, stored, transmitted or received”

**Evidence of the Threat**

There is much evidence and information available to suggest that telephone lines are not secure. A cursory search through the Internet will produce sites specifically intended for ‘phone phreaks’; some even show designs for equipment that could be used to abuse systems. The next section deals with the vulnerabilities of the Fax system.
Threats and vulnerabilities

Facsimile machines present many vulnerabilities which can be exploited either purposely or unintentionally. In either event a disclosure of information may occur, the consequences of which could be extremely serious.

This is quite clearly a long list. They are all real and affect the policy that NHS organisations must adopt to maintain information security as required by our legal, moral and professional obligations.

Dialling

Common mistakes include dialling the wrong number and hitting the wrong speed-dial key. Speed dial keys can be wrongly programmed and could also be set to dial a whole group of recipients.

User error

Modern fax machines have many functions which are accessible to the user. Often the manuals are confusing and crude translations from the native text. An untrained, careless or simply confused user may enter erroneous data which may result in a disclosure of information.

Physical or electronic access to the telephone system

For many years the telephone system has been attacked and abused by so-called 'phone phreaks' who are more than capable of intercepting and diverting phone messages, remotely controlling badly set-up fax machines and forcing events to occur on the lines. An experienced 'phreak' could even intercept a fax, make a copy (or worse, alter it) and send it on to the intended recipient, without the knowledge of either party.

Physical access to the fax machine

It is obvious that a malicious unauthorised user could easily use the machine to his own advantage or gain access to stored documents or printed matter.

Authentication of messages

There is no standard authentication method to verify the source of messages. The various IDs which can be set in the machine can easily be spoofed by an interceptor and could suffer from incorrect or abused entries at the machine. Identification of machines is carried out, normally, by telephone number alone; telephone numbers can easily be spoofed.

Authentication of Features

There is no standard employed across platforms for exchanging authentication details before allowing access to mailbox, store-and-forward, remote functions and polling. Most machines utilise only the phone number for verification.
Encryption
Fax messages are not normally encrypted unless a module has been added. The disadvantage is that to use the encryption, all fax machines involved need to have the same unit fitted.

Confirmation of delivery
Fax machines are connected directly to each other whilst in use. This kind of connection requires no special protocols to confirm delivery; there is no standard protocol to return delivery status messages. The transmission printout confirms only that the message left the machine and entered the phone system with no problems—it does not confirm delivery.

Printers
According to the type of printing mechanism the fax employs, a copy of the message could be held in memory, on a removable film or temporarily on a copying drum.

Modernisation
Many fax machines are now incorporated into photo-copying machines which may be open to further abuses. There are also many fax machines which are connected to computers or sit on a computer network and are therefore subject to all the extra threats specific to computer security.

Polling
It is possible to set modern fax machines to be able to send a set document after receiving a remote request from another machine. An incorrect set-up could allow the first person that called to be sent the waiting document.

Mailboxes
Some fax machines have the capability to store faxes for retrieval by various personnel or to be forwarded automatically or by remote request. A bad setting for the password may allow access to any user.

Quality
Fax machines often produce output of low quality; even a missed decimal point could have disastrous consequences if the data were relied upon for patient care.

Maximum Baseline Information
At all times consideration should be given to the amount of information that is being transmitted. The ONLY identifying details required are the minimum necessary for the recipient to identify the data subject(s).

Obviously this will depend upon many things including the data access items required for the recipient’s access to their own information, the sender’s
confidence in the accuracy of the data and whether the sender is offering other items of identifying data in order to update the recipient’s systems.

We are trying to protect the identity of individuals. We are much more concerned with, for example, the general public gleaning information (whether by accident or not) than we are about healthcare staff. This is not to say we shouldn’t control access within health organisations, as the information should always only be available on a need to know basis.

An identifying code such as NHS number or Hospital number is fairly indecipherable unless the recipient has the decode. Therefore it makes a good basis for the transfer of patient identifiable information.

Caldicott recommends the minimisation of data down to NHS number only. Clearly this will not work if one or other of the parties either doesn’t have access to NHS number, or until all NHS number users have 100% population of the data field.

A sensible alternative maximum baseline would be a combination of the following:

- A code common to both parties (NHS Number, Hospital Number or equivalent)
- Another correlating piece of information to positively identify the data subject such as an element of the Date of Birth or the first three letters of the postcode.

Name should only be used in those circumstances where there are no other common items between the parties.

Address should not be transferred unless critical to the purpose of the transmission.

---

Can I use a fax machine?

The following provides clear guidance on the occasions that use of facsimile machines may or may not be appropriate for the transmission of patient data.

Assessing the need to use fax

When considering the use of fax for transmitting patient identifiable information, the following questions should be asked:

- ‘Do I really need to use a fax?’
- ‘Is it really that urgent?’
- ‘Will normal mail or courier be sufficient?’

Whichever reason is used to justify the use of fax, the principle of minimising the amount of data transferred is to be adhered to. Where possible, irrelevant data is to be blocked out and consideration to be given to passing some items of data over the initial contact call to the recipient.
**Circumstances when the use of fax is acceptable**

Clearly there are certain circumstances when the guarded use of fax for transmitting patient identifying information would be acceptable.

**Harm**

In an emergency, where delay would cause harm to a patient or the potential risk to the patient is greater than the risk of disclosure, the use of facsimile equipment may be considered.

**No alternative**

If alternative, more secure means, such as letter or encrypted electronic mail are not available the use of fax may be considered.

**Agreed concessions where fax may be used**

Notwithstanding the circumstances above, the use of fax for patient identifiable information is not condoned except in defined circumstances including:

- Cancer care urgent referrals
- For cases where alternative methods would not meet with the 0900 deadline for Out-of-Hours reports to be received at GP practices or relevant centres.
- For urgent cases involving the Psychiatric Advisory Service, Emergency Psychiatric Service and Out of Hours teams
- For the timely management of patient transport involving Westcountry Ambulance Services Trust
- For inter-practice urgent referrals
- For the provision of urgent information to a GP from a secondary care provider

These concessions may cease to be necessary when NHSnet is available to all NHS units.

**Circumstances when fax should not be used**

**Sensitive patient information**

Information such as that concerning HIV status, venereal disease, drug abuse, psychiatric history (except in limited circumstances where allowed by the concessions listed earlier), incriminating evidence etc. should **never** be transmitted using facsimile equipment.

**Computer-based facsimile systems**

Computer-based facsimile systems may not be inherently secure. Where strict access controls are not available the system should not be used to transfer patient identifying information. This is especially true where these systems rely on the Internet as a transmission media.
Access and authorisation

Each fax machine should have a nominated person who will be responsible for the equipment. They should also ensure that authorised staff are aware of this policy and are competent in the use of the fax. This person will be referred to as the 'controller' in this document.

The controller, along with the details of the fax, is to be notified to the IT Security Officer (or other designated appropriate person within the organisation) who will maintain a register. Any change of personnel/equipment should also be noted.

Facsimile machines used to transmit patient information should be sited in a secure environment. Access to the equipment should be limited to those people authorised by the controller in the department that the fax serves.

Transmission procedure

Where patient information is to be transferred by fax, the following procedure should be followed wherever possible:

- Prepare a cover sheet that clearly shows who the message is intended for and contact details for the sender. It must be marked ‘Confidential’ and ‘Urgent’ as patient details should only be faxed where there is a pressing requirement. If it isn’t urgent then use another method. An example of a suitable cover sheet is contained in annex A. It should indicate the total number of pages that are being sent to aid verification. It should also bear a message to the following effect:

  “The information in this fax document is confidential and may be legally privileged. It is intended solely for the addressee. Access to this document by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful. If this document is received by anyone other than the addressee, please contact the sender.”

- Unless you are sending details to an unmanned (but securely positioned) fax machine – for example when sending Out of Hours reports to arrive before 0900 to a GP practice - contact the recipient to ensure they are available and to allow them to prepare to receive the Fax within an agreed timescale. During this call you should request that the recipient contacts you should the document not be received within that agreed timescale.

- Take great care in dialling the number, do not rely on your memory, check a reliable and up-to-date source for the number. If the facility exists on the apparatus, double check the ID returned by the Fax station to ensure to the best of your knowledge that it is the correct Fax machine that is answering.

- If speed dialling is to be used, an up-to-date copy of the programmed numbers is to be readily available at the machine. The dialled number is to be monitored if possible.
• Should a published fax number turn out to be incorrect, inform all interested parties of the error and amend the list as necessary.
• If anything appears wrong suspend the call immediately.
• On completion retain the printed record of transmission and include it with a copy of the cover sheet (or the original if you do not require it any more). Give this to the controller for inclusion in the log.

Audit

A logging system should be set up and the log kept for future reference. All confidential faxes sent should be logged. The log should include the following details as a minimum:
• Senders Name
• Sender’s Contact Details
• Date and Time
• Recipient Organisation
• Recipient’s Name
• Recipient’s Telephone Number
• Printout from Fax machine of transmission success
A copy of the cover sheet, which should contain these details, would form the basis of a suitable system.

If it is available, a printout should be requested periodically from the switchboard administrator showing usage of the fax line. This printout should be compared against the usage log. Anomalies should be followed up and corrective action taken where necessary. Should an anomaly represent a threat, or possible threat, to information security, the event should be reported to the IT Security Officer or appropriate authority.

The log should be subject to spot check by the Fax Controller and by the IT Security Officer.

Facsimile machine settings

Each fax machine will have its own functions and settings. To make the transfer of information by fax as secure as possible, the following general considerations should be taken into account when setting up the apparatus.
• The controller should be the only person who is to configure, or to oversee the configuration of the apparatus
• The apparatus should be operated in accordance with the manufacturers’ instructions. The operating manual should be readily available near the machine at all times.
• Speed Dialling should not normally be used. If the use of the facility is critical, numbers are to be checked once entered and a list of numbers is to be available next to the machine for ready reference.

• Should a mailbox system be utilised, the settings should be made so that access is via a password.

• Polling should be disabled so that control of sent items is retained by the sender.

• If the equipment has a remote function access facility, this should be disabled.

## Output handling and sanitisation

• All output which bears confidential information should be handled accordingly.

• No printouts should be left unattended at the fax machine or in the print tray.

• Where the print process uses a transfer film, the film should be disposed of using the confidential waste routine.

• Where the print mechanism employs an image drum (plain paper faxes), a few blank sheets should be printed off to clear the static image held on the drum.

• Where the fax machine houses a memory capability, the machine should have a facility to flush the memory and delete saved items. This facility should be utilised to sanitise the machine at regular intervals.

• Where the facility is part of a ‘smart copier’, extra procedures will be needed to cover any extra functions available. In this case advice must be sought from the Caldicott Guardian.

## Incident reporting

A security incident is defined as any event which has resulted, or could have resulted, in:

• the disclosure of confidential information to any unauthorised individual

• the integrity of the system or data being put at risk

• the availability of the system or information being put at risk

• an adverse impact, for example:
  ♦ embarrassment to the organisation/NHS
  ♦ threat to personal safety or privacy
  ♦ legal obligation or penalty
  ♦ financial loss
  ♦ disruption of activities

It is true to say there are grades of seriousness which can be applied to security incidents. The majority of security breaches are innocent and unintentional, for
example a misdialled number which was noticed before transmission would be a minor occurrence, but the transmission of patient information to the wrong recipient due to a misdialled number would be much more serious in nature.

Staff should report any actual or suspected breaches of security or potential weaknesses in secure operation of any systems, including facsimile equipment.

This report must be made directly to your organisation’s Caldicott Guardian by expeditious means (e.g. e-mail or telephone). The report is made in confidence.
ANNEX A - Example of a cover sheet

COVERING CONFIDENTIAL

URGENT FAX

From: Guy Neecologist
Plymouth Hospitals NHS Trust

Tel: 01752 123456  Date: 35th October 1999
Fax: 01752 123456  Time: 1405

To: Terry Bullsmell
A GP Practice

Tel: 01234 123456
Fax: 01234 123456

Total No of Pages (Including Cover Sheet)  2 Pages

Important Information

The information in this fax document is confidential and may be legally privileged. It is intended solely for the addressee. Access to this document by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. If this document is received by anyone other than the addressee, please contact the sender.

Message starts on next page

COVERING CONFIDENTIAL
Can I Use A Fax to send patient identifiable information?

ASK YOURSELF

- ‘Do I really need to use a fax?’
- ‘Is it really that urgent?’
- ‘Will normal mail or courier be sufficient?’

You can use fax in the following cases

- Cancer Care Urgent Referrals
- Out Of Hours reports for 0900 deadline
- In an emergency where delay would cause harm
- Urgent Psychiatric Services
- Ambulance transport (if req’d)
- Inter-Practice Urgent Referrals
- Urgent transmissions from secondary care bodies to GPs.

Don’t use fax in the following cases

- Very sensitive information (HIV, VD, incriminating info etc.)
- Insecure computer-based systems (esp. Internet)
- Routine matters
- When other methods will do

What is the procedure?

- Prepare Cover Sheet
- Contact Recipient -
  - There to Receive
  - Call-back if not received
- Check Number
- Dial Carefully
- Check Valid Response If Able
- Monitor Transmission
- Suspend If Anomalies
- Obtain Printed Record of Transmission
- Complete Log

Where can I get advice?

Write the contact details of your appropriate advisors here:

Remember - Faxing Can Be Insecure