- Confidential information sent by external mail, must be sent via a secure method where the package can be traced and is signed for on receipt.
- Dispose of personal or confidential information via confidential waste facilities.

Record information accurately and consistently

- Record information onto paper or enter it into the computer as soon as possible.
- If hand writing a record, make sure that it is legible.
- Check individuals' personal details with them to ensure that they are up to date.
- Any alteration or addition on a paper record must be dated, timed and signed.
- Record relevant and useful information. Do not use unnecessary abbreviations or jargon and do not include irrelevant speculation or personal opinions.

Only disclose sensitive information after thought and care

- Confirm the identity of anyone asking for information over the phone (if possible call them back via the switchboard).
- Ask them what they need and why they need it, so you can determine if it is appropriate to provide it to them.
- Respect the sensitivity and privacy of individuals; ensure you are not overheard by others during private phone calls or conversations.
- Establish the patient's wishes with regard to giving information to family and friends.

Using personal information

- Justify why any personal information needs to be used. Seek advice if you need to use any information that could be used to identify a person if you are not dealing with their care directly.
- Only use personal information if necessary and always use the minimum amount of personal information required for the purpose.

When deciding whether to share information

- Ensure that a request is lawful and reasonable either in relation to providing care to an individual patient or working with partner organisations for the good of the public.
- When information needs to be shared about an individual who is not able to give consent and/or has difficulty understanding, ensure that it is in their best interests to do so.
- Make sure you have one of the 'keys to sharing information' (see inside)
- Share the minimum information required to provide the necessary care or to satisfy a lawful, reasonable request.
- Ensure information sharing is timely.

This leaflet sets out your responsibilities when handling personal information. All staff will at some point use personal information and for some this will occur on a day to day basis. Responsibilities for all staff are at the front of this guide. More detailed information for those with a patient-facing role is in later sections

Failure to handle information appropriately may affect patient care, organisational reputation and lead to legal action or a fine. Deliberate inappropriate use is likely to lead to disciplinary action. If in doubt, always seek advice.

www.protectinginfo.nhs.uk

This leaflet is a brief summary of your responsibilities with regard to personal information. If unsure how to handle information, please seek advice or education. Your line manager can direct you, or speak to the Information Governance lead/Data Protection Officer in your organisation.

Developed by the Avon, Gloucestershire and Wiltshire Information Governance Collaboration programme and designed by Avon IM&T Consortium. First published November 2004. Reviewed and updated in January 2008 and October 2010.

Guidance for all staff, volunteers and contractors on handling personal information

Protecting information - protecting people, protecting organisations

Definitions and responsibilities for all staff

Personal information

Information about an individual, which includes either some or all details of their identity is personal and is subject to the Data Protection Act (1998), the Human Rights Act (2000) and other NHS requirements such as the Caldicott principles.

Confidential or sensitive information

Patient information, in any form is confidential. This means that information should only be shared or accessed by someone with a legitimate reason, related to the care of the patient. Information about members of staff or others in relation to sensitive issues, such as appraisals, investigations, complaints or payroll details is also confidential.

Protecting information (including personal and sensitive data)

Keep information secure and available

- Do not share your passwords or smartcards.
- Only access information about individuals where you have a justified work-related reason to do so.
- Only store personal information on electronic media such as a memory stick and always ensure that it is encrypted and only when necessary.
- Ensure that personal information contained in emails is sent by a secure method, either via NHSMail or through approved local procedures.
- Do not leave personal information lying around where it can be seen, read or removed by others.
- A fax message that contains personal information should be sent and received via a 'Safe Haven'. Always confirm the fax number, inform the recipient it is being sent and then check that it has been received. Always send with a cover sheet.
- Patient information or sensitive staff details should be marked as 'private and confidential'.
- Lock record stores and filing cabinets and log-out of computer systems when they are not in use.
- Ensure that if you transport information in any form (paper or electronic), it is kept secure at all times.
- Ensure you are aware of any security requirements when handling information outside of your normal workplace, such as at home or other location. You may not transfer information onto any computer equipment that you own.

Responsibilities for staff with regular access to personal information

Keeping individuals informed about use of their information
Individuals need to know that information about them is being used. You should routinely let them know what you are recording and why. Where there is a need to share information, such as to provide patients with care or monitor quality, individuals should be made aware of this, unless their personal identifiers are removed. Where you have direct contact with the individuals who are the subject of the data you are using, you must ensure that:

- **Leaflets or posters explaining the use of their information are available or offered to individuals.**
- **Where appropriate any correspondence addressed to individuals about their care or services, includes reference to how their information is used.**
- **Individuals are informed when and why their information will be shared amongst staff and organisations providing their care.**
- **Individuals are informed of any choice they have about the use of their information.**
- **Individuals understand what they have been told and have the opportunity to question.**
- **Any request by an individual to see their information, to ask for amendment or to control how it is used, is responded to appropriately and swiftly.**

Consent to use information

For patient care (including children and young people with the capacity to make their own decisions)
As long as patients are informed and understand about the use of their information throughout their care and they do not raise any concerns, then consent to use their information for their care is considered to be implied. It is important to discuss the use of a patient's information with them throughout their care as their views may change.

For other purposes
Where there is a need to use patient information for any purpose other than the provision of their care, several considerations need to be made:

- **Remove all or as many identifiers as possible.**
- **Remove any other detail that is irrelevant to the purpose.**

If enough detail has been removed to make the information anonymous, to the extent that no-one, including the patient could identify themselves, then consent is not necessary. However if identification is needed for the purpose, then a form of consent may be required. For activities such as clinical audits/quality checks, these can be done on the basis of implied consent, by staff caring for the patient or clinical audit staff.

If you need to use identifiable information for activities such as education and research, you must inform the patients concerned and gain their explicit consent. Please seek advice if at all unsure from your Information Governance lead.

Patients who have difficulty in understanding
If an individual has difficulty in understanding how their information will be used, reasonable steps should be taken to explain this to them in a manner that they can understand. The information can be shared if to do so is lawful, reasonable and appropriate. To ensure that you act appropriately, you can take into account the views of other parties who know the individual, such as family or friends. Do not disclose information to individuals where you have concerns that they should not know it. If you need to use information about an individual who has difficulty understanding, for a purpose not related to their care, seek further advice on how to progress.

Responsibilities for staff in direct contact with patients

Managing concerns raised by patients
If a patient raises concerns about how their information is used or shared, then this must be addressed. Take time to discuss their concern and reassure them about how information is handled. Establish whether there will be any impact on their care if information is not used or shared. You must keep a record of care provided in some format. Where a patient has concerns about electronic records, the use of a paper record might be considered, but further support is required. If a patient still has concerns and there is a potential impact on their care, seek further advice from your manager or refer to your Information Governance Lead.

The keys to sharing personal information legally

Information should only be shared for purposes related to the business of the organisation. There are three legal 'keys' that can be used to unlock any sharing situation. You must ensure that at least one applies to the situation before sharing information. Always keep a record of the basis for sharing information.

Key 1 – A legal duty
A number of legal acts create a duty to disclose information. These include the Children Acts (1989 & 2004) with regard to safeguarding, the Terrorism Act (2000), the Road Traffic Act (1988) and communicable disease legislation. Where a legal duty is present, consent is not needed. Individuals should be informed of the sharing, provided to do so will not cause them or anyone else undue harm or distress. Legal duties change, so seek advice if unsure.

Key 2 – A Public or vital interest (a legal power)
In situations where there is no legal duty to share information, the law can permit sharing information without consent, if it can be justified to be in the significant interest of the public or vital interests of an individual and a legal power exists. Examples include prevention of harm, such as vulnerable adults or assisting in criminal cases. The individual(s) should be informed if to do so will not cause any harm or prejudice any situation.

To justify disclosing information in the interest of the public or an individual, you should consider how many people might be affected and the overall impact of sharing. You should consider what might happen if you do share and what might happen if you do not. The more people affected, the greater the public interest, but it is also valid that if a small number of people are significantly affected (either positively or negatively) that too can be considered a public interest.

The vital interests of an individual are generally where sharing information is critical to preventing harm or distress, or is literally a matter of life or death.

Key 3 – Consent
Consent is only valid if the individual has been informed and understands how the information will be used.

Explicit consent: Where the purpose for sharing information is not directly related to their care, then the explicit consent of the individual must be gained, ideally in writing.

Implied consent: Where the purpose is related to their care, then as long as they are aware and understand how their information is being used, and have no objection, consent to share is implied.

So which key?
If there is a legal duty to share, or an overwhelming public or vital interest, to approach an individual to gain consent may be inappropriate as it is likely you will have to share the information anyway. However if there is no legal duty or overwhelming public or vital interest, you must gain an appropriate form of consent (as set out above) to share information.

If you need to share information, and have considered the situation based on this guidance, you will be supported in your decisions. Where possible make decisions with the support of colleagues/managers and get advice from the Information Governance/Data Protection lead or the Caldicott Guardian.