Version 7.0

Information Sharing Core Principles

A set of agreed principles & standards and a framework for developing information sharing protocols.

June 2015

South, Central & West Commissioning Support Unit		
Document status: **Current**		
Version	**Date**	**Comments**
1.0 – 1.5	February 2002	Issued for sign up to organisations
2.0 – 2.5	March 2003	Reviewed and updated – issued for stakeholder consultation
2.6	May 2003	Comments incorporated from stakeholder consultation prior to issue for signature
2.7	Jan 2005	Initial revisions following review group – Jan 2005
2.8	March 2005	Incorporating review group comments, prior to signatory (existing & potential) and patient group consultation.
3.0	May 2005	Incorporate comments from wide consultation – issue for organisational sign up
3.1	March 2007	Re-drafting of document along principles discussed by Avon, Gloucestershire, Wiltshire Information Governance Forum, prior to stakeholder workshop in April 2007
3.2	April 2007	Revised following comments and discussion during stakeholder workshop, prior to issue for comment
3.3	May 2007	Revised following consultation with stakeholders, prior to issue to relevant organisations and groups representing interests of individuals/members of public
4.0	July 2007	Incorporate final stakeholder & representative group comments, prior to active distribution
4.1	April 2010	Draft revision commenced in 2009 for consultation
5.0	June 2010	Comments from consultation incorporated and issued for organisational sign up.
6.0	August 2012 (issued December 2012)	Regular review – issued for stakeholder consultation in October 2012
7.0	June 2015	Biennial review

June 2014

Development facilitated by South, Central & West Commissioning Support Information Governance (Adam Tuckett – Head of Information Governance). Contribution from all signatories.

If you need further copies of this document or in a different format please telephone Adam Tuckett on 0117 900 2410

http://www.protectinginfo.nhs.uk

1 Purpose, overview and management:

Information sharing is a key enabler for the provision of effective services to individuals particularly where a co-ordinated approach across agencies is required. If poorly managed this contributes to a failure to provide effective services, the potential to suffer a damaging loss of data, confidentiality breaches and privacy concerns for individuals. This has been validated by the second Caldicott report (April 2013) establishing a new principle that 'it can be as important to share information as to protect it.'

Information sharing between agencies is often defined in a framework of three levels:

1. At the top level, a shared and documented commitment to key principles, standards and purposes between organisations.
2. At the middle level functional agreements defining the information to be shared, how it will be shared and when
3. At the third level, for frontline staff, tools and methods for actual sharing (ref https://www.gov.uk/government/publications/information-sharing-for-practitioners-and-managers).

This document sets out the top level commitment by all participating agencies to adhere to the principles, standards and directions defined within it. The commitment covers the sharing of personal information in any form by any method, including verbal, paper, recorded and electronic formats. This document applies to sharing between organisations and professionals. It does not cover communication between professionals and patients/service users, or carers.

The aim is to promote a consistent approach to the sharing of information that will benefit individuals and services whilst protecting the people that information is about. It has been developed from a core 'sharing agreement' used across the Avon, Gloucestershire and Wiltshire communities since 2003.

This set of principles will be reviewed every two years, or at the request of any organisation using the document if there is a concern over the document's fitness for purpose, or when there is a change in governing legislation.

The document has been reviewed in line with the Information Commissioner's Data Sharing Code of Practice (May 2011). The ICO code of practice is a statutory document and whilst organisations cannot be in breach of the code, it is noted that to not follow the code is likely to put organisations in breach of the Data Protection Act (1998). It has also been further revised in line with the second Caldicott report, regulations for processing personal data for commissioning and proposed changes from the forthcoming EU Data Protection regulation.

2 Does personal data need to be shared?

Key principle - inclusion of any data that might identify an individual must have a legal basis, be justified and agreed as both necessary and proportionate to achieve the purpose(s).

Any activity to share data must first consider if 'identifying personal information' is required and if so to what degree. Information can generally be put into two categories, depending on what it is being used for.

- Information shared to benefit the individual or others, usually requiring clearly identifiable data. This is mainly related to the provision of 'direct care'. This is defined by the Caldicott report as: 'clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and alleviation of the suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care'. Please note 'direct care' itself is NOT a legal basis for sharing data and a suitable legal basis, such as consent, duty or public interest must be in place.

- Information shared for the benefit of the public or sections of society. Such information is often used to inform decision making or planning. It may range from completely anonymous statistics to raw datasets that include items of data that relate to a greater or lesser degree to individuals' identities. This is often 'not direct care related' as defined in the Caldicott report as: activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which falls outside the scope of direct care. It covers care services management, preventative medicine and medical research. Examples of activities would include risk stratification, service evaluation, needs assessment and financial audit'.

The starting point will be that a 'privacy-friendly' approach will be adopted by any process for sharing information; therefore the inclusion of any data that might identify an individual must be justified and agreed as both necessary and proportionate to achieve the purpose(s).

2.1 Sharing clearly identifiable data (generally for direct care purposes)

Key principles

- **Data must only be shared if there is a legal duty, an overriding public interest/vital interest of the individual or a basis of consent to justify the exchange.**
- **Individuals must be informed about data sharing unless there is a robust reason not to inform them.**

Sharing of personal/sensitive information must be done 'fairly' and 'lawfully'. The legal basis for sharing is set out in the Data Protection Act (1998), common law duty of confidentiality and the Human Rights Act (1998). In simple terms 'lawful' sharing requires consent from the individual, unless there is:

- A legal duty to share information set out in specific legislation, such as the Children Act (1989, 2004), Road Traffic Act (1988) and others.
- A legal power to share information where sharing without consent can be justified by a robust public interest, or in the vital interests of an individual.

Legal duties, robust public interests and vital interests are related to conditions in the Data Protection Act (1998) and are recognised practice in the common law of confidentiality.

In addition sharing must be 'fair' by ensuring the subject is aware of what is being shared and for what purpose. Only in situations where informing the subject is likely to cause them or others significant harm/distress, or prejudice actions or outcomes of a situation, can this principle be set aside. If an individual lacks the capacity to make a decision, they should still be informed in an appropriate manner if possible.

It is also useful to reference the 7th Caldicott Principle as set out in the second Caldicott report (2013) 'The duty to share information can be as important as the duty to protect it' when considering the basis for sharing data.

Deciding the basis of justification:
*'*Second level' sharing protocols developed in relation to these core principles will detail how information is to be shared 'fairly and lawfully' by consideration of each of the following options, in order, documenting and justifying the approach to be taken:

1. **Use of explicit consent**, unless it is not legally required and is judged by all parties involved to be clearly impractical. *(It is legally required for sharing sensitive information where no other condition in schedule 3 of the Data Protection Act (1998) such as 'medical purposes', 'vital interests' or 'legal duty', can be applied.)*
2. **Use of implied consent**, where explicit consent is not being used and reasonable measures have been undertaken to inform subjects of the activity and an agreed process to manage objections is in place.
3. Reference to specific legislation which sets a **duty to share**, related to the purposes covered by the specific protocol which makes consent unnecessary.
4. Reference to specific **legal powers** relevant to the purposes for sharing, including consistent approaches to justify public or vital interests to sharing without consent.

'Second level' sharing protocols will detail processes for informing subjects about what is being shared and why. Where necessary they will include potential justifications for not informing subjects. These must be related to appropriate provisions in the Data Protection Act (1998) such as 'Crime & Disorder exemptions' (section 29(3)) and 'Statutory Instruments/modification orders *'where allowing access would be likely to cause serious harm to the physical or mental health or condition of the subject or any other person'*.

Note – The Data Protection Act does not apply to information on deceased individuals but general principles of common law and Human Rights should still be applied.

2.2 Sharing for administration, management, planning and developing services where there is a need to include some identity factors

Key principles:

- **Information shared for planning and developing services must only contain identifying items if absolutely required, and only the bare minimum required.**
- **If after removing as much identifying information, one or more identifying factors remains, the principles relating to justifying the sharing of identifiable data (section 2.1) must be adhered to.**
- **Careful attention to regulations governing the control of personal data in health and social care commissioning must be taken into consideration (refer to the current regulations at the time the sharing is proposed).**

Information is classed as 'personal' and subject to the Data Protection Act if it relates to a living individual who can be identified from those data, or from other information, which is in the possession of, or is likely to come into the possession of the data controllers. Any second level sharing protocol which shares statistical information for planning purposes should not include any identifying information such as name, identity number, date of birth and addresses without a robust and documented legal justification for the use of each item of data.

Where information relating to ages of individuals is required, consideration will be given to using age brackets/groups. If age brackets are not appropriate, the smallest amount of data on the date of birth will be used that will satisfy the purpose. Often the year of birth will suffice. Where a purpose requires information on addresses of individuals, a part postcode will be used, unless more accurate location information is required. Full postcodes should only be used where absolutely required and where advice has been taken from Information Governance specialists. Many uses of full postcode when combined with other data make the data set identifiable, requiring adherence to the principles in section 2.1. In addition some postcodes relate to just one property.

Any extraction of data that includes potentially identifying information and especially where the extraction features small numbers of cases (counts of less than 5 records), should be referred to the Data Protection Leads of the organisations concerned to ensure that the data in either raw or combined state does not identify individuals, or if identification is at all possible, that compliance with Data Protection principles is in place.

2.3 Anonymous/pseudonymised data – shared for planning, developing services

Key principle:

- **If data is truly and permanently anonymised it can be shared provided it relates to the legitimate business of the partner agencies. Whilst legal requirements are not so stringent it is good practice to only share relevant and required information.**
- **Additionally if data has been pseudonymised it can be shared with other agencies who do not have the 'key' to reverse the pseudonyms**

If the data to be exchanged does not in anyway identify individuals and cannot be combined with any other data that would lead to the identity of individuals, then, provided the organisations sharing the information are acting within the range of activities they are legally set up to do (their 'vires'), information can be shared. **In situations where data is to be shared on an ongoing basis, especially where the sharing will be relatively frequent, then a specific exchange agreement is required.**

3 Justifications and related purposes for sharing information

The table below sets out high level purposes and potential justifications for sharing personal information based around the requirements of the Data Protection Act (1998).

If a purpose is not listed it does not mean that information cannot be shared. 'Second level' sharing protocols should add relevant detail of the legal powers organisations have to undertake activities that require sharing of information. In addition the levels described below are starting points for consideration, it is possible that in relation to any purpose there could be a situation where a different justification is made. The column for either direct care or secondary use is based on definitions from the Health & Social Care Information Centre: (http://www.hscic.gov.uk/article/3638/Personal-data-access-FAQs#General%20questions)

Overall purpose(s):	**Initial justification**	**Initial level of identity**	**Direct Care/ Secondary Use or public interest**
Delivering routine care and treatment across agencies	Consent of the individual. Between healthcare providers this can be implicit; with external agencies it may need to be explicit.	Identifiable data generally required – second level protocol may not be necessary	Direct Care
Safeguarding & protecting vulnerable individuals – including: Where emotional, physical, sexual, psychological, financial, material or discriminatory abuse/neglect is suspected, a crime committed or regulations breached.	If gaining consent would delay or put individuals at increased risk, information can be shared on the basis of 'vital interests' of the individual(s). In situations relating to children, many organisations have a legal duty to co-operate, which is interpreted as a duty to share relevant information. For adults there is not the same legal basis at present, so consent is the starting point	Identifiable data generally required – second level protocol/document may be required – which may reference national guidance on such matters	Direct Care
Prevention & detection of crime and the apprehension and prosecution of offenders, including terrorism	Consent is the starting point unless agreed by parties that informing and consenting may be reasonably likely to prejudice the situation. In certain circumstances a legal duty may apply such as terrorism cases and road traffic incidents.	Identifiable data generally required – Second level protocol likely to be necessary.	Public interest linked
Assuring and improving the quality of care / treatment	Where sharing is between agencies involved in healthcare, then this can be based on implied consent and legitimate management of healthcare services. For specific cases explicit consent should be sought unless there is an agreed reason not to.	Identity should be removed entirely or reduced to an absolute minimum. Specific documentation on the purpose, basis and legal justification required.	Local clinical audit – direct care. Other uses are secondary.

Managing and planning services. Monitoring and protecting public health. Contracting for services	If any identifiers are required then there must either be a consent, legal duty, section 251 approval in place to permit the sharing.	Identity should be removed entirely or reduced to an absolute minimum. Specific documentation on the purpose, basis and legal justification required.	Secondary use
Emergency planning & preparedness	Reference to be made to Cabinet office guidance on Formal Information Sharing under the Civil Contingencies Act 2004 and 'Data Protection Sharing guidance for Emergency Planners and responders', noting that duties to share do not override the Data Protection Act 1998. Consent can be used and should be considered, but may be impractical. Disclosure in the public interest may be necessary and it may also be in the vital interests of individuals.	Limited personal or sensitive personal information should be used for emergency situations. Planning and testing may well be possible without using identifiable data. Specific sharing documentation at the second level is likely to be required.	Public interest linked

4 Organisational responsibilities (Data Protection Compliance & 'Caldicott'):

All organisations sharing data must ensure that they have adequately addressed all of the following responsibilities and be prepared to assure sharing partners of their compliance, when entering into a sharing agreement.

- Organisations must actively inform individuals of how their information may be used and to whom it may be disclosed by provision of appropriate materials in a variety of formats and through contact with staff. It must highlight their rights to access, withhold and correct information and provide details of the process for individuals to access their records.
- Organisations must complete and maintain a Data Protection notification detailing all sources, subjects, purposes and disclosures relevant to their business and partnerships under any agreement.
- Organisations must maintain the accuracy and clarity of data they supply to aid usefulness and consistent interpretation. Where necessary, partner organisations will be informed of any changes to the data they have received and also notify the source of any error they discover. A key item for accuracy is use of a consistent shared identifier, such as the NHS number, so that information shared is linked to the correct individual. The Health & Social Care (Quality & Safety) Act 2015 and subsequent regulations support and promote the use of the NHS number as the consistent identifier for health and adult social care. It should also be used where possible and legitimate for childrens services.
- Organisations must ensure that collection and sharing of information is necessary and proportionate to the purpose(s), and neither excessive or inadequate.
- Organisations must maintain the confidentiality of data in any form, during collection, transmission and storing with appropriate security arrangements and general compliance with ISO27000.
- Specific agreements will detail the security requirements, but as a minimum these will include access by encrypted link, transfer by encrypted email or encrypted removable media/mobile devices (where encrypted email is not possible or sharing is taking place in person)
- Organisations will apply relevant regulations to the retention & disposal of records, only keeping information for as long as is necessary in relation to the original purpose(s) for which it was collected.
- Organisations will ensure all staff are educated to manage information appropriately in line with these principles and organisational policy on the collection and uses of information, supported by contractual terms of employment.
- Organisations should ensure that access to shared information is on a strict 'need to know' basis and is justified either by consent or another legal basis for accessing the information. Onward sharing with 3rd parties will also be managed on the 'need to know' and legal justification basis and where possible the original source(s) should be informed.
- Organisations will ensure that any 3rd parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements.
- Organisations will have processes/systems for recording wishes/restrictions on information expressed by individuals.
- Organisations in receipt of a 'Freedom of Information' request that covers personal data, such as staff information, provided by another organisation, will discuss the

situation with the other organisation prior to disclosure and aim to develop a consensus view on any potential exemptions.

5 Indemnity & non compliance:

At the level of principles and standards adopted by organisations there will not be any indemnity between organisations relating to actionable situations arising from information sharing. The need for indemnity should be assessed in second level protocols. Organisations will complete a compliance statement (overleaf) that should be provided to any sharing partner on request. Should a partner have concerns over the level of compliance, they should address these with the relevant organisation. The organisational 'data controllers' are responsible for assessing the risk of sharing information with any organisation where compliance is limited. This assessment should be based on the risk to information from sharing compared with the risk to the fulfilment and quality of the purpose information is to be shared for. Any serious disputes should be referred to the office of the Information Commissioner.

6 Second level documentation:

Each service/initiative basing sharing on these principles, is responsible for creating procedure documentation detailing how information will be shared securely, and how the principles have been applied including how sharing can be audited. Where required this will be a specific 'Second level' protocol, with appropriate guidance and process documentation.

When is second level documentation required and what should it look like?
Second level documentation is often required to achieve some (or all) of the following:

- Consistent and agreed approach to the exchange of data with clarity over responsibilities for the confidentiality, quality, security and availability of data
- Agreement on specific legislation, directions, standards and guidance relevant to the subject/initiative.
- Set out specific data items to be exchanged, the frequency, the security requirements and the agreed methods of exchange or access.

It is a fair question to ask if 'second level' documentation is required. There is no specific rule to determine, but as a guide, routine sharing on a recognised care pathway (such as GP referral to secondary care) will not require a protocol whereas situations that diverge from a care pathway (such as alerting to a safeguarding issue) may well do, as will cross organisational data sharing for planning & development purposes.

Second level documentation can be set out as one of a number of document types, including:

- Shared organisational policy and procedure – for example sharing information on vulnerable adults is best documented as an intrinsic part of an overall cross organisational shared policy and procedures on supporting vulnerable adults.
- Specific information sharing agreement – typically used where an initiative requires specific data to be shared between identified agencies/contacts within a stipulated timeframe and is extracted, compiled and securely transferred. (Data Push)
- System access agreement – typically where the data to be shared is enabled by providing access to it within an information system to partner organisations. This will define how system access controls are to be applied, how users are to be

managed and how any issues/incidents will be handled as well as any specific detail required around the sharing.

- Governance arrangements for integrated/shared services – where staff are to formally work together in at least a partially integrated manner, the core governance documentation around such services must reference the relevant information resources and the access and control of them.

.

Second level documentation will feature the following unless clearly not required:

- The perceived benefits, to any party, related to the purposes for sharing the information. To be described as clear objectives and include processes to review appropriateness or agree further purposes
- Description of the legal basis for sharing relating to the purpose(s) including specific context legislation, noting any duties, powers or obligated controls on information and including Data Protection conditions relied upon.
- Clear detail of the level of identity used in the sharing of data (where applicable) and where necessary assessing the level of identity from activity to combine sets of data – where individual data sets may not be identifiable, but become so when combined.
- The level of detail required in the data to be shared, ensuring it is the minimum required for the purpose and a process to determine and agree if more detail becomes necessary.
- How data subjects will be informed of the sharing of data unless legal exemptions are applicable. Where the data sharing is expected, then a privacy notice accessible to individuals may be sufficient. Where it is not expected specific informing activity is likely to be required.
- A commitment to accuracy and completeness of data exchanged, including a process for informing all relevant parties of any inaccuracies identified
- Agreement to the process for exchange, taking account of threats and vulnerabilities in the proposed communication methods and ensuring adequate and agreed safeguards to protect the information during transit and storage are in place, including as a minimum robust encryption of data transferred electronically.
- Agreement to the period of retention of data – with reference to organisational retention schedules.
- Agreed destruction processes relevant to the nature of the information (i.e. confidential shredding/deletion).
- Description of the timescale and frequency of exchange of data
- A process for managing breaches of security, inappropriate disclosure of data and loss of data

7 Organisational compliance statement

The following activities must be undertaken to comply with responsibilities set out in this document. Each organisation using this document is required to indicate whether relevant activities are in place or in development. In completing the statement, reference should be made to appropriate organisational policy, process and guidance documentation. Completion should be by the Organisation's nominated Data Protection Officer/Information Governance lead. Each signatory must store their own statement and be able to provide it to another signatory on request.

Organisational responsibilities:

Responsibility area	**In Place?** **In Progress/target date?**
Keeping subjects informed	
▪ Active provision of information to patients/service users of the uses to which information about them may be put and to whom it may be disclosed.	
▪ Publicise and implement processes to provide access to records to subjects on request	
Provide choice	
▪ Have policy covering consent to use information and respond to any specific requests made by subjects with regard to handling their information	
Protect information	
▪ Have documented policy and processes to check the accuracy and clarity of data both with the subject and on information systems	
▪ Protect the confidentiality and security of data in any form, during collection, storage and sharing with appropriate security arrangements (generally compliant with ISO27000 Information Security Management standard) – via relevant policy, process and staff guidance on handling information ▪ Have facilities to encrypt data sent via email, placed on removable media, or stored on mobile devices	
▪ Documented policy and process relating to retention and disposal of information & equipment	
▪ Ensure contractual arrangements with staff (employment terms), contractors and other suppliers/individuals handling identifiable information contain reference to confidentiality/non disclosure, secure data handling and destruction	
▪ Provide education and training to all staff on the safe handling of personal data including sharing/disclosing information. ▪ Control access to shared information on the 'need to know basis'	
▪ Complete and maintain a Data Protection notification detailing all sources, subjects, purposes and disclosures relevant to their function and partnerships under any agreement	

Monitoring	
• Have incident and risk reporting arrangements that incorporate information related issues • Audit & assess security of information flows and information systems • Perform regular (at least annual) assessments and audits of organisational compliance with legislation and regulation on processing personal information	
Organisation Name & contact details:	

Appendix 1: Second level protocol headings example:

INFORMATION SHARING: SECOND LEVEL PROTOCOL FOR ……

BETWEEN ……

1. Purposes & benefits of information sharing

2. Role & Responsibilities of Partners

- Can include definition of who are 'data controllers'
- If required reference to process to agree other purposes
- Commitment to accuracy and timeliness of sharing
- Commitment to legal compliance items such as access to records by the subject

3. Relevant Legislation, standards and guidance including:

- Description of the processing conditions relied upon in the Data Protection Act
- Description of other relevant legislation that either permits or requires data sharing or places specific controls over use and sharing of personal data.

4. Approach to consent, legal duty or legal powers to share with reference to:

- Process for informing subjects (or reason for exempting this activity)

5. Information exchanged or shared between partners

- Reference to level of identity and justification for identifiers being included
- If required the defined dataset
- Process for reporting and dealing with inaccuracies
- Agreed periods of retention

6. Security – covering methods of exchange and storage including:

- Physical security
- Electronic security (access control, encryption)
- Managing breaches of security
- Agreed periods for retaining data and methods for confidential destruction

7. Complaints Procedures

8. Awareness Training/communication to involved individuals

9. Monitoring & Review

10. Glossary of terms and abbreviations

Example Information exchange agreement:

	DATA TRANSFERRED BETWEEN:	**AND:**	**AND:**
NAME			
ADDRESS			

PURPOSE/REASON for TRANSFER/ACCESS The legal framework relating to the purpose(s) for sharing information. Agreed purposes for the use of information and a process for agreeing further purposes if necessary	
DATA TYPE **e.g. patient, staff, business/finance** Refer to the level of identity used in the sharing of data and where necessary assessing the level of identity from combined sets of data.	
DATA DESCRIPTION	
DATABASE(S) USED **e.g. PMS, Pathology, Radiology**	
CONSENT/LEGAL BASIS The legal basis for sharing information, in relation to the initiative, based on consent or other legal justifications for sharing. How individuals will be informed of the sharing of data where required	
PHYSICAL TRANSFER METHOD **e.g. Memory Stick, Network access, NHSNet, Laptop PC** Agreement to the process of exchange, taking account of threats and vulnerabilities in the proposed communication methods and ensuring adequate safeguards to protect the information during transit and storage are in place.	
SOFTWARE FORMAT USED **e.g. Word, Excel, CSV, etc.**	
ENCRYPTED or UNENCRYPTED	
QUALITY A commitment to accuracy and completeness of data exchanged, including a process for informing all relevant parties of any inaccuracies identified	

SECURITY A process for managing breaches of security, inappropriate disclosure of data and loss of data	
DATE and TIME OF TRANSFER or commencement if ongoing	
FREQUENCY IF ONGOING	
RETENTION Agreement to the period of retention of data – with reference to organisational retention schedules and the longest applicable period, unless there is reason for destruction of copies of data.	
MONITORING Who will monitor that the processes above are taking place and are effective? What checks will be made?	
INCIDENT MANAGEMENT & RESOLUTION PROCESS How will any breaches of principles be reported and managed? What will be the procedure to update this protocol in the light of any findings?	

I the undersigned certify that the personal data being received will not be disclosed to unauthorised persons. The Data and their Purposes of Use are Notified under the Data Protection Act 1998 and my organisation/company is committed to compliance with the Data Protection Principles.

DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	
DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	

Copy to: Information Governance Officer

PROCEDURES FOR ENSURE SAFE TRANSFER OF INFORMATION

Every member of staff has an obligation to request proof of identity before confidential personal information is passed on.

Every member of staff is personally responsible to take precautions to ensure the security of confidential personal information both whilst it is in their possession and when it is being transferred from one person or organisation to another.

The following is a list of recommended procedures to ensure the safe transfer of information:

- Envelopes should be securely sealed, clearly addressed to a known contact and marked "confidential" and "addressee only". A return to sender address should also be marked on the envelope[1].
- Telephone validation, or "call back" procedures should be followed before disclosing information to someone you do not know to confirm their identity and authorisation[2]. Fax transfer is not safe and should be avoided wherever possible. Where it is necessary "Safe Haven"[3] procedures should be followed.
- Data held on removable media/disk should be encrypted and the physical security of the device should be protected i.e. kept under lock and key. The encryption password must be kept separate from the device. Any external agencies used to create device must use individual passwords for each device.
- E-mailing patient confidential information is only permitted if it is encrypted[4] or where system-to-system networks are known to be secure.
- Confidential patient information **must not** be transmitted via the Internet without it being encrypted.
- When anonymised or pseudonymised[5] information is shared, care should be taken to ensure that the method used is effective and individuals cannot be identified from the limited data set e.g. age and postcode together could be sufficient enough to reveal an individuals identity.

1 The NHSIA recommend a return "post-box" address is used to avoid revealing the identity of the sender where this may compromise confidentiality.

2 The details of the caller and the agencies published telephone number (not direct dial or mobile phone numbers because they cannot be validated) should be obtained, checked against directories and a telephone call made back to check authenticity.

3 Safe Haven Requirements (EL (92) 60) – An agreed set of administrative and physical security procedures for ensuring the safe and secure handling of confidential patient information including locked rooms and special arrangements for the transit of records and correspondence

4 Encrypted – information in plain-text format is converted into characters and codes using privacy enhancing technology so that it cannot be understood if intercepted in transit, the recipient de-codes it.

5 Anonymised information is data with all personal identifiers stripped out; it can neither reveal the identity of the individual concerned nor link back to that person – even if it became necessary at a later stage. Pseudonymised data is where one key is left in order to link back to an identity if there is a need to do so e.g. a numerical identifier.