Information Sharing Protocol

derbyshire partnership forum

Version	4.0
Date	4 April 2016
Author	Arden and GEM CSU and Derbyshire County Council
Document Owner	Derbyshire Partnership Forum
Approving Committee	Derbyshire County Council Information Governance Group, Derbyshire Information Governance Network, Derbyshire Partnership Forum
Review Date	April 2018
Document Classification	PUBLIC

Change History

Version	Date	Description of change
3.5	December 2015	Draft
3.6	January 2016	Comments from Mel Turvey, Derbyshire County Council
3.7	February 2016	Comments from David Gurney, Derbyshire County Council
3.8	March 2016	Comments from Information Governance Group, Derbyshire County Council and Arden and GEM CSU
3.9	March 2016	Comments from Derbyshire County Council and Arden and GEM CSU
3.9.1	March 2016	Formatting and comments from Mel Turvey, Derbyshire County Council
4.0	April 2016	Agreed by Information Governance Group, Derbyshire County Council, Derby City Council, Derbyshire Community Health Services NHS Foundation Trust and Arden and GEM CSU

Contents

1. Why do we need a Protocol to share information?

The Derbyshire Partnership Forum is committed to working together, putting the individual at its heart for the improved planning and delivery of Derbyshire's public services, safeguarding and to promote the welfare of children and adults.

To work well in partnership, we need to share information, including sensitive personal data, between individuals, professions and organisations – including public, private and voluntary sectors. Effective and structured sharing of information between partners has the ability to inform care and planning, allows us to understand trends and patterns of activity, to respond to emergencies appropriately, and to support the lives and safety of individuals, families and communities. At a time when the gathering and storing of information continues to increase, we have a moral and statutory responsibility. We need to be able to share information carefully and responsibly and to assure service users, patients, carers, practitioners, providers, the public and partners that information held about them or from their organisation is shared securely and appropriately, whilst also respecting an individual's right to privacy and confidentiality. Effective use of information will support us in achieving all the ambitions and aspirations we have for those living in Derby and Derbyshire.

All organisations should play a role in supporting the sharing of information between and within organisations and address any barriers to information sharing to ensure that a culture of appropriate information sharing is developed and supported.

This document sets out the overarching principles and commitments that will underpin the secure and confidential sharing of information between organisations involved in delivering services to people living and working within Derby and Derbyshire and contains a template to create an Information Sharing Agreement **(see Appendix 8)** between yourselves and other organisations within the Partnership.

2. Structure

The overarching Information Sharing Protocol outlines the principles and standards of expected conduct and practice of the signatories and their staff and applies to all sharing of sensitive personal and non-personal information. The Protocol establishes the organisations' intentions and commitment to information sharing and promotes good practice when sharing personal information. It also contains the legislative standards that all types of personal information sharing must comply with.

3. Aims and objectives of the Protocol

The purpose of this overarching Protocol is to set out a framework for partner organisations to manage and share information on a lawful and 'need to know' basis with the purpose of

enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.

Specifically, this Protocol aims to:

- Set out the general principles of information sharing
- Identify the lawful basis for sharing information
- Set out generally what information will be shared
- Define the common purposes for holding and sharing data
- Set out how information will be stored.

This Protocol applies to chief officers, executive directors, non-executive directors, trustees and all employees including volunteers and agency staff of the organisation and partner organisations who are signatories.

The Protocol also applies to any organisation or agency which has been commissioned to deliver services on behalf of any organisation party to this Protocol where permission has been given to the third party organisation to disclose information.

The Protocol is intended to complement any existing professional Codes of Practice that apply to any relevant profession working within any organisation, and does not constitute legal advice.

4. What does the Protocol cover?

4.1 Data sharing

By ‘data sharing’ we mean the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;
- exceptional, one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation making data available to each other.

Some data sharing does not involve personal data, for example where only statistical data that cannot identify anyone is being shared. Neither the Data Protection Act (DPA), the Information Commissioners (ICO) Code of Practice nor this Protocol, apply to that type of sharing provided that an individual cannot be identified – see especially par 4.3.2 below.

There are two main types of data sharing:

4.1.1 Systematic data sharing

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

4.1.2 Exceptional data sharing

The majority of data sharing takes place in a pre-planned and routine way and this Protocol sets out the principles for effective information sharing and the establishment of Information Sharing Protocols. However, organisations may also decide, or be asked, to share data in situations which are not covered by any routine agreement i.e. one-off decision to share data for a range of purposes. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

Different approaches apply to these two types of data sharing and this Protocol and resulting Information Sharing Agreements need to reflect this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing. In either case however, the sharing of personal data must comply with the requirements of the legislation.

4.2 Who can we share data with?

Data can be shared within organisations, with partner organisations as a 'Data Controller' and with third parties as a 'Data Processor'.

4.2.1 Sharing with a 'data controller'

The DPA and ICO define a data controller as "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed." The majority of instances where data is to be shared under this Protocol and any Information Sharing Agreements are predominantly about sharing personal data between data controllers.

4.2.2 Sharing with a 'data processor'

As mentioned above the Protocol and Information Sharing Agreements are predominantly about sharing personal data between data controllers. However, there is a form of data sharing where a data controller shares data with another party that processes personal data on its behalf and the DPA and ICO identifies these organisations as 'data processors'.

A data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller; and
- it has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle, **see Appendix 2**.

Therefore a data processor involved in data sharing does not have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller.

4.2.3 Sharing within organisations

Data sharing and the data protection principles also apply to the sharing of information between the different departments of an organisation such as local authority or financial services company. An approach and willingness to share information across departments should be encouraged to support the needs of the wider organisation whilst adhering to the principles and requirements set out within this Protocol.

4.3 Types of data to be shared

The Protocol applies to the following types of data:

4.3.1 Personal, sensitive personal data and personal confidential data (PCD)

The Data Protection Act (see **Appendix 2**) identifies two types of data Personal and Sensitive personal data, both relate to living people (Data Subjects). However the Caldicott Information Guardian Review (**See Appendix 3**) identified a third classification of Personal Confidential Data (PCD), which relates to both living and deceased individuals.

i) Personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Such data could include the data subjects name, address, medical or bank details.

ii) Sensitive personal data Certain types of personal information have been classified as sensitive data, the Data Protection Act 1998 (which relates to living individuals only) provides that additional conditions must be met for that information to be used and disclosed lawfully. The term 'sensitive' data refers to information that provides details of racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or mental health, sexual life, commission or alleged commission of an offence, criminal proceedings or sentence.

iii) Personal confidential data (PCD) describes personal information about identified or identifiable individuals which should be kept private or secret and refers to any information held either as manual and/or electronic records, or records held by means of audio and /or visual technology, about a living or deceased individual who can be personally identified from that information. Examples of identifiable data are Name, address, postcode, date of birth, NHS number.

4.3.2 Anonymised and Pseudonymised information

Information that falls into this category is data about people that has been aggregated, tabulated or has had unique identifier replaced or removed in ways that make it impossible to identify the details of individuals. This can be shared without the consent of the individuals involved and the processing is outside the provisions of the Data Protection Act 1998. However, care should be taken to ensure that it should not be possible to identify individuals either directly or in summation. This can happen when anonymised information is combined with other data from different organisations, where the aggregated results produce small numbers in a sample, or where traceable reference numbers are used. Further guidance on anonymised information and requirements can be found in the Information Commissioners Office 'Code of Practice on Anonymisation'.

4.3.3 Non-personal information

Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

There is a general presumption and expectation that anonymised and non-personal information will be shared, unless there are exceptional reasons for this. These may include:

- commercial confidentiality;
- where disclosure may forfeit the organisations duty to ensure safe and efficient conduct of organisational operations;
- policy formulation (where a policy is under development and circulation would prejudice its development);
- protect other legal and contractual obligations; and
- where information is marked protectively (refer to your organisations standards for information classification for further details).

5. The Information Sharing Protocol Principles

This Protocol recognises that sharing of information should be done fairly and lawfully, be properly controlled and should strike a balance between the specific rights of individuals and the public interest. The following are the principles to be applied whenever personal confidential information is shared or exchanged. The organisations signed up to this Protocol are fully committed to ensuring that these principles are adhered to at all times.

The principles established by this Protocol are:

- Information about individuals will only be shared when and where it is needed.
- Information will be shared in accordance with statutory duties, underpinned by specific protocols and information sharing agreements where appropriate;
- Information that is provided in confidence will be treated as confidential;

- Information will only be used for the purposes for which it was collected and shared;
- Individuals will be properly informed about the way their personal information is used and shared and told if it changes;
- Consent to share personal information will be sought wherever appropriate;
- Considerations of confidentiality and privacy will not automatically cease on death;
- The information rights of individuals will be respected and observed;
- Organisations collecting personal information will publish service-specific privacy statements and all sharing agreements.

To achieve these principles, Partner organisations agree to:

- Share information with each other where it is lawful and when they are required to do so, for more information please see the flowchart of key questions to information sharing in **Appendix 6**;
- Adhere to the legal framework governing information sharing, see **Appendix 1**
- Comply with the requirements of the Data Protection Act (DPA) 1998, in particular with the 8 Data Protection Principles, see **Appendix 2** and to register with the Information Commissioner's Office (ICO), if the organisation processes personal information (unless exempt).
- Share information in accordance to all the 7 Caldicott principles, see **Appendix 3**
- Inform individuals when and how information is recorded about them and how their information may be used;
- Ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer;
- Develop local Information Sharing Agreements **Appendix 8** that govern the way transactions are undertaken between partner organisations and with other organisations that are not parties to this Protocol;
- Promote staff awareness of the Protocol and any relevant Information Sharing Agreements and ensure that staff have had the appropriate level of training in information security and confidentiality;
- Promote public awareness of the need for information sharing through the use of appropriate communications media;
- Ensure external accreditations are achieved such as level 2 of the Information Governance (IG) Toolkit, PSN and/or ISO27001;
- Share information and ensure patient/citizen confidentiality by embedding the 5 rules into organisational systems and processes as set out by the Health and Social Care Information Centre see **Appendix 4**.

These may be supplemented by additional specific legislation such as the Health and Social Care (Safety and Quality) Act 2015

6. Commitments in support of the Protocol

Signatories to this Protocol are committed to the implementation of an appropriate level of Information Governance throughout their organisation, in accordance with recognised national standards. They will:

- Adhere to the principles and commitments of this Protocol whenever exchanging personal information, whether with a co-signatory or other agency/organisation;
- Share statistical and anonymised/pseudonymised data wherever possible, eliminating the use of personal information except where reasonably necessary;
- Ensure that all staff (including temporary employees, contractors and volunteers) are aware of and comply with their responsibilities arising from both the Protocol and relevant legislation, and receive adequate training in order to do so;
- Implement their own policies on confidentiality, data protection, information security, records management and information quality, which are appropriate to their organisation and comply with recognised codes of practice.

Establish efficient and effective procedures for:

- Obtaining, informed consent to collect, share and process personal information wherever reasonably practicable;
- Informing citizens and/or patients what information they collect and share about them;
- Sharing of personal information identified as part of a detailed agreement;
- Addressing complaints arising from the misuse or inappropriate disclosure of personal information arising from information sharing decisions;
- Enabling access to records of individuals by those individuals on request;
- Amending records where they have been shown to be inaccurate and informing partners where these are shared;
- Review and destroy information in accordance with good records management practice and organisational policy;
- Sharing information without consent when necessary, recording the reasons for that disclosure (including legal basis) and the person responsible for making the decision;
- Making information-sharing an obligation on staff and allocating senior staff responsibility for making complex disclosure decisions;
- Ensuring that personal information is protected at all times, through the use of appropriate protective marking, security and handling measures;
- Develop and work to detailed, specific information sharing agreements that support identified purposes;
- Ensure that future developments in technology reflect the requirements of the Protocol and any detailed protocols that support it;
- Issues, incidents and complaints resulting from failures in the specific agreements will be fed into the review processes for the individual protocols;

- Share information free of charge unless special charging arrangements have been agreed;
- Seek legal advice where appropriate;
- Ensure their registration as Data Controllers under the Data Protection Act 1998 is adequate for the purposes for which they may need to process and share information with one another;
- Support the principles of equality and diversity within the community and ensure that whenever information is provided to the public it will be supplied in appropriate formats and languages as appropriate.

7. Purposes for which information will be shared

Each of the signatory agencies, their staff and representatives, agree to share information between them, to the extent that is fair and lawful. Information will only be shared for a specific lawful purpose or where appropriate consent has been obtained (see section 8).

Organisations are responsible for providing a culture of support to ensure that good practice in information sharing is promoted and supported.

The following range of purposes are agreed as justifiable for the transfer of personal confidential information between the partner agencies as defined within the remit of this Protocol:

Organisations aim to establish:

- A culture that supports information sharing between and within organisations including proactive mechanisms for identifying and resolving potential issues and opportunities for reflective practice.
- A systematic approach to explain to service users when the service is first accessed, how and why information may be shared.
- Clear systems, standards and procedures for ensuring the security of information and for information sharing.
- Infrastructure and systems to support secure information sharing, for example, access to secure email or online information systems.
- Effective supervision and support in developing practitioners and managers professionals' judgement in making these decisions.
- Mechanisms for monitoring and auditing information sharing practice.
- Designated source of impartial advice and support on information sharing issues, and for resolution of any difference of opinion about information sharing.
- There is an established information sharing governance framework so that staff are clear about the organisations position on information sharing.
- Information sharing governance framework must always recognise the importance of professional judgement in information sharing at the front line and should focus on how to improve practice in information sharing within and between agencies.

8. Obtaining consent to share

Partner organisations/staff can share information about Data Subjects (patients, people), which is relevant to their care. Wherever possible, consent should be sought and practitioners and providers need to be open and honest with the individual (and/or their family, where appropriate) from the outset as to why, what, how and with whom, their information will be shared.

8.1 Sharing with consent

The Information Governance Review, March 2013, defined Consent as:

8.1.1 Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

8.1.2 Explicit consent is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care.

8.1.3 Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent **(see Appendix 7 for more information on the Direct Care Model).**

Consent should also be obtained where an individual may not expect their information to be passed on and they have a genuine choice about this. Consent in relation to personal information does not need to be explicit – it can be implied where to do so would be reasonable i.e. a referral to a provider or another service. More stringent rules apply to personal confidential data, when, if consent is necessary then it should be explicit.

8.2 Sharing without consent

Consent is not always needed to share personal information**.** Without consent, or explicit consent, it is still possible to share personal information if it is necessary in order to carry out your role, or to protect the vital interests of the individual where for example, consent cannot be given, or where it is unsafe or inappropriate to do so; for example, where there

are concerns that a child is suffering, or is likely to suffer significant harm, consent would not be needed although a record of your decision and what has been shared should be recorded.

Where personal confidential information needs to be shared in order to fulfil statutory requirements, these requests will be considered and approved by the appropriate Caldicott Guardians or Senior Information Risk Officers (SIROs) of the partner organisations.

Staff should seek advice where necessary from their organisation's Data Protection Officer/Information Governance Manager.

For further guidance on consent, please see **Appendix 5,** and for further guidance on the decisions needed to share information and obtain consent see the flowchart and accompanying notes in **Appendix 6.**

9. Sharing with organisations who are not signatories to this protocol

Any organisation who is not party to this overarching Protocol, but who wishes to share information may do so, providing that there is an existing Information Sharing Agreement or contract in place with the third party, that they agree to comply with the terms of this overarching Protocol and have adequate technical and non-technical security arrangements in place, for example compliance with the Information Governance Toolkit.

10. Implementation, Monitoring and Review

The Protocol is owned by all of its signatories. The intention has been to develop an over-arching code of behaviour for all information-sharing applications. This will be supplemented by Information Sharing Agreements for specific purposes which will adopt the principles and commitments in the Protocol as their base line and identify any additional service specific requirements.

Work to develop individual agreements will be the responsibility of the organisations wishing to share information

The Protocol will be reviewed two yearly and will be updated to account for any changes in legislation and developments in national guidance. Issues arising from breaches of the Protocol, changes in legislation, or recommendations arising from review may result in an earlier review.

Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the Protocol and publishing any individual Information Sharing Agreements they may have.

Any of the signatories can request an extraordinary review at any time when a joint discussion or decision is necessary to tackle local service developments.

11. Breach of Confidentiality

All agencies who are party to this Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or unintentional.

In the event that personal information shared under this Protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- Inform the organisation who provided the data of the details;
- Take steps to investigate the cause;
- Take disciplinary action against the person(s) responsible, if appropriate;
- Take appropriate steps to avoid a repetition;
- Take appropriate steps, where possible, to mitigate any impacts.

On being notified of a breach, the original information provider along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose information has been compromised, and if necessary will:

- Notify the individual(s) concerned;
- Advise the individual(s) of their rights; and
- Provide the individual(s) with appropriate support.

Where a breach is identified as serious, it may have to be reported to the Information Commissioner's Office. The original Data Controller (information provider), along with the breaching organisation and others as appropriate, will assess the potential detriment to individuals, volume of data, and the sensitivity of data subject of the breach, and, identify and agree appropriate action.

12. Complaints

Partner organisations must have in place procedures to address complaints relating to the inappropriate disclosure of information. The partner organisations agree to cooperate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.

If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

13. Organisational and individual responsibilities

Disclosure of personal confidential information without consent must be justifiable on legal/statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act 1998. Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act 1998 or damages for a breach of the Human Rights Act 1998. A full list of the exemptions can be found at the website of the Information Commissioners Office:

http://www.ico.org.uk/for_organisations/data_protection/the_guide/exemptions

13.1 Individual responsibilities

Every employee working for the organisations listed in this Partnership Agreement:

- is personally responsible for the safekeeping of sensitive information they obtain, handle, use and disclose
- should know how to obtain, use and share information they legitimately need to do their job
- has an obligation to request proof of identity, or take steps to validate the authorisation of another before disclosing sensitive information
- must uphold the general principles of confidentiality, follow the rules laid down in this Protocol and seek advice when necessary
- should be aware that any violation of privacy or breach of confidentiality is unlawful and may be a disciplinary or criminal matter that could lead to their dismissal or prosecution.
- should ensure any information is transferred using an approved, secure method of transportation in accordance with their organisation's policies and procedures

Every employee working for the organisations listed in this Protocol must ensure they follow their own organisation's policies and procedures before releasing any information under this agreement.

13.2 Organisational responsibilities

Each partner organisation is responsible for making sure that their organisational and security measures protect the lawful use, confidentiality, integrity and availability of information shared under this Protocol.

- Partner organisations will accept the security classifications on information and handle the information accordingly.
- Partner organisations accept responsibility for auditing compliance with the information sharing agreements in which they are involved.

- Partner organisations should make it a condition of employment that its employees will abide by its rules and policies on the protection and use of confidential information.
- Partner organisations should make sure that their contracts with external service providers abide by their rules and policies on the protection and use of confidential information.
- The partner organisation originally supplying the information should be notified promptly of any breach of confidentiality, or incident, involving a risk or breach of the security of information.
- Partner organisations should have documented policies for records retention, maintenance and secure waste destruction.

14. Protocol Signatories

Members of the Derbyshire Partnership Forum (DPF) have agreed to abide by the terms of this Protocol, its appendices and any variations to the Protocol or its appendices. The latest list of DPF members is available on the Derbyshire Partnership Forum website as well as the updated list of signatories to this Protocol.

http://www.derbyshirepartnership.gov.uk/about_us/

Appendix 1 - Legal Framework and Categories

General Legal Framework

The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.

The purpose here, therefore, is to highlight the legal framework that affects all types of personal information sharing, rather than serve as a definitive legal reference point.

The general legal framework surrounding the sharing of information includes:

- United Kingdom Administrative Law (the law that governs the actions of public bodies);
- Human Rights Act 1998 and the European Convention on Human Rights (Article 8.1);
- Health and Social Care (Safety and Quality) Act 2015
- Data Protection Act 1998;
- Freedom of Information Act 2000;
- No secrets, Department of Health 2000;
- Common Law Duty of Confidence;
- Caldicott Principles 2013;
- Children's Act 1989, 2004;
- Crime and Disorder Act 1998;
- Education Act 1996, 2002, 2005, 2011;
- Health Act 1999, 2006, 2009;
- Care Act 2014;
- Mental Health Act 1983, 2005, 2007;
- Mental Health (Patients in the Community) Act 1995;
- National Health Service and Community Care Act 1990;
- NHS Information Governance Framework (IG Toolkit)
- Government Security Classifications April 2014; and
- Legislation that covers specific aspects of public service delivery (e.g. child protection, patient records).

Overall the law strikes a balance between the rights of individuals and the interests of society. The law is not a barrier to sharing information where there is an overriding public interest in doing so (such as where it is necessary to do so to protect life or prevent crime or harm) provided it is done fairly and lawfully.

Often personal information can be shared simply by informing people from the outset what purposes their information will be used for and then sharing only for those agreed purposes.

There are however special legal considerations around sharing information that is personally sensitive or confidential, because this could have serious consequences for individuals. In deciding whether the law allows personal information to be shared, the following four steps should be considered (as recommended by the Ministry of Justice):

1. Establish whether there is a legal basis for sharing the information (i.e. whether the reason for sharing the information has a statutory basis – eg the prevention of crime) or whether there are any restrictions (statutory or otherwise) to sharing the information;

2. Decide whether the sharing of the information would interfere with human rights under the European Convention on Human Rights;

3. Decide whether the sharing of the information would breach any common law obligations of confidence;

4. Decide whether the sharing of the information would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles, which are that personal information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with individuals' rights
- Secure
- Not transferred to other countries without adequate protection

Further detailed guidance on using personal and sensitive personal information fairly in accordance with the Data Protection Act 1998 is set out in **Appendix 2.** In addition, the Freedom of Information Act 2000 gives anyone (an individual or an organisation) a right to request access to information from a public body. Where an exemption applies (e.g. it is third party personal information or commercially sensitive information), disclosure may be refused.

Appendix 2 - Data Protection Principles

The Data Protection Act 1998 governs the protection and use of personal data. It sets out standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by the 8 Data Protection Principles. Under the key principles of the Act, personal data must be:

Principle 1 - processed fairly and lawfully. There should be no surprises – data subjects should be informed about why information about them is being collected, what it will be used for and who it may be shared with;

Principle 2 - obtained and processed for specified purposes. Only use personal information for the purpose(s) for which it was obtained and ensure it is not processed in any other manner that would be incompatible with that purpose(s);

Principle 3 - adequate, relevant and not excessive. Only collect and keep the information you require. It is not acceptable to collect information that you do not need. Do not collect information 'just in case it might be useful one day';

Principle 4 - accurate and kept up to date. Have in place mechanisms for ensuring that information is accurate and up to date. Take care when inputting to ensure accuracy and have local procedures in place to manage requests for information to be amended;

Principle 5 - not kept for longer than is necessary. The legislation within which area you are working in, will often state how long documents should be kept. Information should be disposed of in accordance to your organisation's Records Management Policy (including retention and disposal);

Principle 6 - processed in accordance with the rights of the data subject under the Act. These rights include the right to:

- Make subject access requests;
- Prevent the processing of data which is likely to cause them substantial damage or substantial distress;
- Prevent processing for the purposes of direct marketing;
- Be informed about automated decision making processes that affect them;
- Prevent significant decisions that affect them from being made solely by automated processes;
- Seek compensation if they suffer damage or distress through contravention of the Act;
- Take action to require the rectification, blocking, erasure or destruction of inaccurate data;
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

Principle 7 - protected by appropriate security. This involves:

- ensuring the confidentiality of faxes by using Safe Haven /secure faxes;
- keeping confidential papers locked away;
- ensuring confidential conversations cannot be overheard;
- ensuring information is transported securely;
- good information management practices;
- guidelines on IT security;
- procedure for access to personal data;
- retention and disposal policies for confidential data;
- processes to ensure secure deletion of electronic data.

Principle 8 - not transferred to a country or territory outside the EEA without an adequate protection.

If sending information outside the EEA, ensure informed consent is obtained from the individual and that there is an adequate level of protection for the rights of the individuals whose personal data you are transferring. Consider carefully what is posted on websites or sent via email and obtain approval from the data controller.

Source: Data Sharing Code of Practice – Information Commissioners Office

https://ico.org.uk/for-organisations/guide-to-data-protection/

Appendix 3 - Caldicott Principles

The Caldicott Review 2013 re-enforced the original principles of 1997 regarding the use of client information in health and social care organisations and added a 7th principle regarding the sharing of information.

- **Principle 1 - Justify the purpose(s)**

  Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

- **Principle 2 – Do not use personal confidential data unless it is absolutely necessary**

  Person confidential data items should not be included unless it is essential for the specified purpose (s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose (s).

- **Principle 3 -Use the minimum necessary personal confidential data**

  Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

- **Principle 4 -Access to personal confidential data should be on a strict need to know basis**

  Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may been introducing access controls or splitting data flows where one data flow is used for several purposes.

- **Principle 5 -Everyone with access to personal confidential data should be aware of their responsibilities**

  Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6 - Comply with the law**

  Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

- **Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality**

  Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Source: https://www.gov.uk/government/publications/the-information-governance-review

Appendix 4 - HSCIC Guide to Confidentiality

The Health and Social Care Information Centres 'A Guide to Confidentiality in Health and Social Care 2013' sets out that there should be no surprises about how confidential information about individuals is used and the 5 rules set out how the obligations are to be fulfilled:

Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully.

Rule 2: Members of a care team should share confidential information when it is needed for safe and effective care of an individual.

Rule 3: Information that is shared for the benefit of the community should be anonymised.

Rule 4: An individual's right to object to the sharing of confidential information about them should be respected.

Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

Guide to Confidentiality; Health and Social Care Information Centre 2013

http://www.hscic.gov.uk/confguideorg

Appendix 5 - Consent: Guidance notes

Consent

For consent to be valid, it must be:

- fully informed – the individual is aware of what information will be shared, with whom and for what purpose, and who controls the data (data controller);
- specific – a general consent to share information with 'partner organisations' would not be valid. Specific means that individuals are aware of what particular information we will share, who with and for what purpose;
- freely given – the individual is not acting under duress from any party.
- the individual must have capacity to give consent

Individual organisations may have their own procedures for dealing with issues of implied/explicit consent in order to allow it to meet its lawful obligations. Staff should refer to organisational procedures.

The person giving the consent must also have the capacity to understand what they are consenting to.

To give valid informed consent, the person needs to understand why their information needs to be shared, what type of information may be involved, who that information may be shared with and the possible consequences if it is not shared (if relevant).

The person should also be advised of their rights with regard to their information namely:

- the right to withhold their consent
- the right to place restrictions on the use of their information
- the right to withdraw their consent at any time
- the right to have access to their records.

In general, once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent. However, it is best practice for practitioners to review this regularly.

If a person makes a voluntary and informed decision to refuse consent for their personal confidential information to be shared, this decision must be respected unless there are sound legal grounds for disclosing without consent. The consequences of not providing consent should be explained, e.g. such as not receiving the right treatment or service/amount of support.

New consent will be required where there are to be significant changes to:

- the personal data that will be shared,
- the purposes for which it will be shared, or
- the partners involved in the sharing (i.e. the proposed data sharing is not covered by the original fair processing notice).

Capacity to consent

For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process. See guidance as defined in the Mental Capacity Act 2005.

Young Persons - Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent. The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent. This is augmented by the Fraser (previously Gillick) Competency test.

It should be seen as good practice to involve the parent(s) or guardian/representative of the young person in the consent process, unless this is against the wishes of the young person. In the case where the wishes of a young person, who is deemed competent to give consent, are opposed to those of their parent/carer, then the young person's wishes should take precedence.

Recording consent - all agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

The consent form should indicate the following:

- details of the agency and person obtaining consent;
- details to identify the person whose personal details may/will be shared;
- the purpose of sharing personal information;
- the organisation(s) with whom the personal information may/will be shared;
- the type of personal information that will be shared;
- details of any sensitive information that will be shared;
- any time limit on the use of the consent;
- any limits on disclosure of personal information, as specified by the individual;
- details of the person (guardian/representative) giving consent if appropriate.

The individual or their guardian/representative, having signed the consent, should be given a copy for their retention. The consent form should be securely retained on the individual's record and relevant information should be recorded on any electronic systems used, in order to ensure that other members of staff are made aware of the consent and any limitations.

Disclosure without consent

Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act 1998. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability.

There are exceptional circumstances in which a patient's right may be overridden, for example:

- if an individual is believed to be at serious risk of harm, or
- if there is evidence of serious public harm or risk of harm to others, or
- if there is evidence of a serious health risk to an individual, or
- if the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime, or
- if instructed to do so by a court.

In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

Legislation which permits the sharing of data without consent includes:

- NHS (Venereal Diseases) Regulations 1974
- Notifications of Births and Deaths Regulations 1982
- Codes of Practice, Mental Health Act 1983, s 1.3 – 1.13 and s 14
- Police and Criminal Evidence Act 1984
- Public Health Act 1984 and Public Health (Infectious Diseases) Regulations 1998
- Children's Act 1989 s 47
- Abortion Regulations 1991
- Finance Act 1994
- VAT Act 1994, s 91
- Criminal Procedure Investigation Act 1996
- Social Security Administration (Fraud) Act 1997
- Audit Commission Act 1998
- Crime and Disorder Act 1998, s 115
- Data Protection Act 1998, schedule 2 and schedule 3
- Terrorism Act 2000 s 19
- Civil Contingencies Act 2004

All agencies should designate a person(s) who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person(s) should hold sufficient seniority within the organisation with influence on policies and procedures. Within the health and social care agencies it expected that this person will be the Caldicott Guardian.

If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

A record of the disclosure will be made in the patient's record and the patient must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed.

If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection work) where it may not be appropriate to inform the patient of the disclosure of information.

This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the patient of such disclosure. In many such situations it will not be a case of never informing the patient, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the patient's record, clearly stating the reasons for the decision, and the person making that decision.

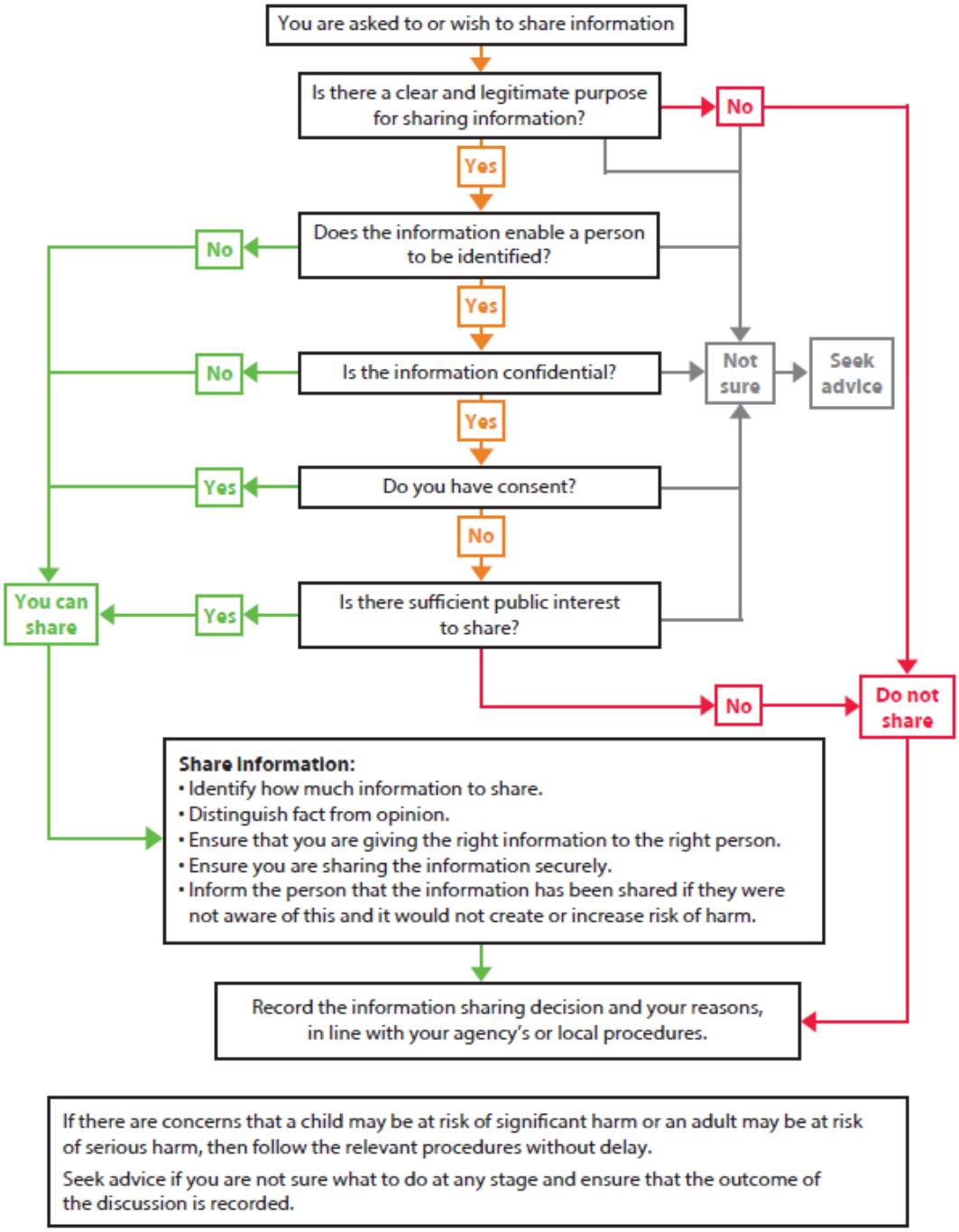
Further Reading on consent to share information

Information: To share or not to share? The Information Governance Review https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Information Commissioners Office (ICO)

https://ico.org.uk/for-the-public/personal-information/sharing-my-info/

Appendix 6 - Flowchart of key questions for information sharing



Source: HM Government 'Information Sharing: Guidance for practitioners and managers

https://www.education.gov.uk/publications/standard/Integratedworking/Page1/DCSF-00807-2008

Explanation of some of the flowchart sections:

These explanations are taken from HM Government 'Information Sharing: Guidance for practitioners and managers. The full explanations have not been included in this document and so please also refer to the full Guidance, available at:

https://www.education.gov.uk/publications/standard/Integratedworking/Page1/DCSF-00807-2008

- Is there a clear and legitimate purpose for sharing information?

  Whether you work for a statutory or non-statutory service, any sharing of information must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is an important part of meeting those requirements.

- Does the information enable a living person to be identified?

  If the information is anonymised, it can be shared. However, if the information is about an identifiable individual or could enable a living person to be identified when considered with other information, it is personal information and is subject to data protection and other laws.

- Is the information confidential?

  Confidential information is:

  - personal information of a private or sensitive nature; and
  - information that is not already lawfully in the public domain or readily available from another public source; and
  - information that has been shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others

  This is a complex area and you should seek advice if you are unsure.

- Do you have consent to share?

  Consent issues can be complex and a lack of clarity about them can sometimes lead practitioners to assume incorrectly that no information can be shared. Page 17 of the guidance document (link above) gives further information to help you understand and address the issues. It covers:

    - What constitutes consent
    - Whose consent should be sought; and
    - When consent should be sought

- Is there sufficient public interest to share the information?

  Even where you do not have consent to share confidential information, you may lawfully share it if this can be justified in the public interest. Seeking consent should be the first option. However, where consent cannot be obtained or is refused, or where seeking it is

inappropriate or unsafe, the question of whether there is a sufficient public interest must be judged by the practitioner on the facts of each case. **Therefore, where you have a concern about a person, you should not regard refusal of consent as necessarily precluding the sharing of confidential information.**

A public interest can arise in a wide range of circumstances, for example, to protect children from significant harm, protect adults from serious harm, promote the welfare of children or prevent crime and disorder. There are also public interests, which in some circumstances may weigh against sharing, including the public interest in maintaining public confidence in the confidentiality of certain services.

- Are you sharing information appropriately and securely?

  If you decide to share information, you should share it in a proper and timely way, act in accordance with the principles of the Data Protection Act 1998, and follow your organisation's policy and procedures.

- Have you properly recorded your information sharing decision?

  You should record your decision and the reasons for it, whether or not you decide to share information. If the decision is to share, you should record what information was shared and with whom.

Appendix 7 - Direct Care Consent Model

How is Direct Patient Care defined?

The Caldicott Review defined it as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of 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.

How is Indirect Patient Care defined?

Defined by the Caldicott Review 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 fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit.

The Direct Care Consent Model is particularly to support improvements in the delivery of unplanned and emergency care as well as in the delivery of care in the community aimed at preventing admissions. In order to provide quality, safe care, it is necessary for clinical colleagues to be able to view elements of a patient's record during a consultation. This access is for the purposes of direct care by those who have a legitimate relationship with the patient, and who are seeing the patient in a face-to-face consultation.

Principles:

1. Sharing information with care professionals involved in the patients/citizens direct care is essential to provide high quality care. Information can be shared either by capturing explicit patient consent or by setting implied consent supported by the legal and professional duty to share information.

2. Patients/citizens have a right to object to information sharing and unless this would result in significant harm to the patient or others this should generally be respected.

3. Where information systems only allow for the whole record to be shared (with limited entries marked as private) or nothing to be shared; decisions can be made about what mechanisms should be used to share information to support direct patient/citizen care.

4. A professional decision can be made to set implied consent (supported by the duty to share information) to make the patients/citizens information available in order to satisfy the care needs of patients/citizen.

5. The users of the information or data must have a legitimate relationship with the patient/citizen i.e. they are part of a team providing direct care to the patient/citizen who are bound by the duty of confidentiality.

6. The users must be either 'registered or regulated professionals' or, in the case of administrative and support staff, be directly supervised by registered or regulated professionals as part of the wider care team, as per Caldicott2 Review recommendations.

7. The model for consent and sharing patient information across organisational boundaries must be communicated appropriately with patients/citizen, who may provide an objection to sharing.

8. Often there is no "perfect" model that can be realistically implemented in a timely fashion without detracting from the best possible care for the patient. In these cases a risk based approach may be taken considering a number of key pieces of advice; the 7 Caldicott Principles, the ICO Data Sharing Code of Practice/Checklist and Health and Social Care Information Centre Guide to Confidentiality. A Privacy Impact Assessment must be carried out where there are significant changes to use of data, for example, changes in provider and in other cases as specified by the ICO Privacy Impact Assessment Code of Practice and other regulatory bodies.

9. Explicit consent should be overwritten when it is in the Patient/Citizens vital interest or there is a statutory obligation to do so.

10. The use of explicit and implied consent will vary from service to service and is demonstrated in the table below.

Organisational Setting	**Consent model**
Primary Care (GP) Record	• Implied consent 'set' for GPs to access data made available by other SystmOne users. As the GP has overarching responsibility for care (share in). • Implied consent 'set' to share out the GP record with others; this should be appropriately communicated* to patients indicating that the implemented process within SystmOne is that explicit consent to view the GP record must be captured by the other service consuming the information. • *Communication should include posters in the practice, leaflets, included on practice websites and included in practice privacy/fair processing notices.
Emergency Care	• Explicit consent captured to access data made available by others, communicated appropriately to patients (share in). • Implied consent 'set' to make data available to others (where it can be captured) (share out). Consider here your duty to share information.

Organisational Setting	Consent model
Out of Hours	• Explicit consent captured to access the records made available by others (share in) and implied captured to make information available to share (share out).
Community Nursing Services	• Explicit consent captured to access the records made available by others (share in). • Implied consent 'set' to make information available to others (share out).
Non Nursing Community Services (e.g. health promotion)	• Explicit consent captured to access the records made available by others (share in) and implied consent is 'set' to make information available to share (share out).
Secondary Care (including out-patient services)	• Explicit consent captured to access the records made available by others (share in) and implied consent captured to make information available to share (share out).
Social Care	• Explicit consent captured to access the records made available by others (share in) and implied consent captured to make information available to share (share out).
Other organisations	• Explicit consent captured to access the records made available by others (share in) and implied consent captured to make information available to share (share out). • Or where statutory duty allows sharing without consent

Appendix 8 - Information Sharing Template

Insert Organisational Logo(s)

[Information sharing agreement – name of agreement]

Information Sharing Agreement Template

Version	
Document owner	
Document author and enquiry point	
Document authoriser	
Review date of document	
Document classification	
Document distribution	
Document retention period	
Next document review date	

All Information Sharing Agreements must be sent to [the organisation] Information Governance Department for initial review and registration.

Contents

9. Access and Security

Explain the standards and conditions which are required to protect the information concerned. Include any special arrangements which might apply. For example access to files will be restricted – operate a clear desk policy, employees given access on a need to know basis.

10. General Operational Guidance

Include or reference any general operational guidance which is relevant to the purpose of the agreement that is not covered in any other section. Details of relevant contacts can be appended to the document.

11. Management of the Agreement

Additional information should be provided to address:-

- Handling of complaints or breaches of the agreement
- Handling of requests for information under Data Protection/FoI
- Appropriate Signatories
- Review of the Agreement
- Compliance with the Agreement
- Closure/termination of agreement