Barnet Partnership Information Sharing Protocol

Barnet Partnership Information Sharing Protocol

Contents

1 Background

Public services are increasingly being provided by more joined up and integrated agencies

The balance needed in order to share information for the purpose of providing an efficient and effective service and that of ensuring the protection and privacy of individuals is one that needs to be appropriately managed.

Whilst public authorities must safeguard the information they hold, often the needs of the public are best served by the sharing of information between public sector agencies and their Partner Organisations where it is appropriate to do so. In addition to supporting the provision of care, sometimes it is only when information held by different organisations is pulled together that a person is seen to be in need of additional or alternative services. Sharing information, therefore, is a key element to the delivery of high quality, cost effective and seamless services.

It is necessary that all Partner Organisations concerned have a clearly defined framework to facilitate the sharing of personal data whilst respecting the rights of the individuals. The purpose of this framework is to facilitate that exchange of information between services effectively, fairly and lawfully and to provide a single, managed, clear and joint approach to exchanging information.

The creation of an agreed overarching Information Sharing Protocol (ISP), supplemented by appropriate Information Sharing Agreements (ISAs) that define specific areas of the information sharing in detail, provides the basis for this framework.

1.1 The need to share information

Improved information sharing is integral to a partnership approach to service delivery and will lead to improved practice in many areas involving cross team or service working. Good public sector information sharing can benefit our service users in the following ways:

- Case work is supported with information; the provision of high quality services requires the right information to be available to the right person at the right time.
- Helps us achieve our strategic objectives; joined up working between Partner Organisations to achieve strategic aims across the area.
- Good practice is shared on ‘what works’; increasing services’ effectiveness by Partner Organisations learning from each other.
- Evidence is provided to support local policy making.
- Open Data is published to improve transparency and enable maximum value from information.
- Help for people to live their own life.
- A greater understanding and awareness of “what matters” most to people.

- Easier access to information, advice and knowledge.
- Greater awareness and use of the most appropriate resources and assets. Improved access to the most appropriate practitioner or service provider.
- Improving the health of people in the local community. Protecting and supporting people in need.
- Coordinated assessment and provision of care and support across organisations.
- Joint visits and less duplication of the questions we ask people.
- In care, reduction of unscheduled admissions to hospital, residential and nursing homes.
- Improved managing, planning and communication between key organisations.
- Identification of a support network including key relationships.

The Data Protection Act (DPA) 1998, along with the common law of privacy and other EU and English law directives, provides a framework to ensure that personal data about living individuals is shared appropriately – it should not be seen as a barrier to sharing information, but a way of ensuring it is done correctly with the protection of individuals paramount in the decision making.

Organisations should however understand that refusing to share information can also be a risk. Deliberately failing to share data where the law allows a clear gateway to do so can be detrimental to the public and the delivery of services and best outcomes.

Information sharing is crucial to wholly understand a person's needs and is key to more joined up ways of working, multi-agency working, and a more personalised experience for the individual. At a higher level sharing insight leads to better policy making and resource management. Sharing information therefore is a major element in the delivery of high quality, cost effective and seamless public services.

2 Scope

The purpose of this Information Sharing Protocol is to provide a robust framework for the exchange of information between Partner Organisations effectively, fairly and lawfully. It will provide a single, clear, joint approach to exchanging information, reducing the duplication of work, and ensuring we work together more effectively.

Whilst an ISP is not contractually binding it sets out good practice and standards to ensure compliance with legal responsibilities governing the sharing of personal data. Adherence to these standards will help to remove barriers to effective information sharing. This Protocol takes account of the principles and recommendations for sharing information provided in the Information Commissioner's Data Sharing Code of Practice.

Whilst the emphasis within the Protocol is largely on the use and protection of personal data, the general principles should also be adopted when dealing with commercially sensitive information.

This Protocol covers the two main types of data sharing as defined by the Information Commissioner's Office:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

There are many accepted bench marks for an organisation to utilise in gaining an understanding of their current compliance levels. In care, the NHS Information Governance Toolkit (IGT) provides a mechanism for organisations to assess their information governance performance against agreed national standards. All parties to this agreement are encouraged to utilise these services where available and appropriate to assist them with achieving an adequate level of Information Governance performance (i.e. attainment of Level 2 or above against all requirements of the NHS IG Tool Kit).

Organisations that are able to demonstrate that they have achieved the required level of information governance performance can be referred to as Trusted Organisations. Sharing between Trusted Organisations is simplified as there is already a minimum level of information governance in place. This protocol does not seek to replace the requirement for organisations to demonstrate their achievements, nor does it reduce the requirement on individual organisations to maintain suitable levels of information governance achievement, but it does serve to provide a mechanism for those organisations that have yet to achieve the required level of information governance achievement to confirm their commitment. In addition this protocol will ensure transparency and reassurance to service users, clients and patients that their personal information is being shared and protected properly.

This document will provide direction and guidance with information sharing law and standards. It must be underpinned by individual subject-specific Information Sharing Agreements (ISA) to establish a more binding relationship for specific data sharing initiatives.

Each underpinning ISA will set out the technical and practical arrangements and legal basis for sharing, relevant to that particular sharing arrangement. All agreements will need to be compliant with this Protocol and an ISA template has been developed to support this.

For the purpose of this Protocol the term “data” and “information” are interchangeable. The Protocol outlines levels of data sensitivity and an agreed set of principles under which each level of information will be shared and used. Information sharing may involve reciprocal exchanges between organisations, or the pooling of data.

2.1 Types of information

2.1.1 Level 1 – Non personal / Open data

Following central government’s drive to make the public sector more transparent to citizens, Partner Organisations should pro-actively publish as much information as possible. Once information has been identified as Level 1, the expectation is that Partner Organisations will make this information publicly available.

Level 1 information is information that:

- does not identify specific individuals, either by itself or in conjunction with other information in the public domain;
- does not fall under any exemptions or exceptions in the Freedom of Information Act 2000 and Environmental Information Regulations 2004; and
- is not subject to a formal information sharing agreement made under this protocol.

2.1.2 Level 2 – Non personal / Depersonalised / Psuedo-anonymised data

Non-personal, depersonalised or pseudo-anonymised information is data in a form where the identity of the individual cannot be determined. To comply with this the Data Controller must ensure that:

- all identifiers and/or references which could lead to an individual being identified are removed; and
- the information being shared cannot be combined with other information held by the Partner Organisation which in turn may result in the individual being identified.

Level 2 information which is truly anonymised is no longer personal data and therefore should be used where possible. Sharing between Partner Organisations should still be limited for the purposes of the enquiry.

Commercially sensitive data is also categorised as Level 2. Commercially sensitive is defined in Section 43 of the Freedom of Information Act as a trade secret or where release of the information is likely to prejudice the commercial interests of any person (a person may be an individual, a company, the public authority itself or any other legal entity).

2.1.3 Level 3 – Personal data

The sharing of personal and sensitive personal data is governed by the Data Protection Act (DPA) 1998. Sharing personal and sensitive personal data is not an automatic assumption and there must be a clear purpose, for example achieving an objective or set of objectives that can only be achieved by way of sharing personal data.

The Data Protection Act (DPA) 1998 defines 'personal data' as information relating to a living individual who can be identified either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

All Partner Organisations must agree that they may only share Level 3 data within the constraints of the following guidance:

- a person's full name is an obvious likely identifier; but other information such as a customer reference number, address, written or verbal description, photograph, voice recording or CCTV image could also identify them;
- Partner Organisations need to consider whether the sharing of personal and sensitive personal data is absolutely necessary in order to achieve their objective (e.g. can the objective be achieved by sharing anonymised data);
- Level 3 information will be shared on a case by case basis and where it is necessary for information to be shared. Personal data will be shared only on a need-to-know basis where a clear legal justification exists;
- personal data will only be shared when the disclosing Partner Organisation is satisfied that the sharing complies with the Data Protection Act 1998, the Human Rights Act 1998 and any other EU or English legislation; and
- Partner Organisations should only share Level 3 information with one another under agreed and signed information sharing agreements drafted in accordance with ICO guidance and this Information Sharing Protocol.

Sensitive personal data is personal data along with information classified by the DPA as a sensitive characteristic. DPA legislation applies a high level of security and high threshold of acceptable use if the information falls into the category of sensitive personal.

Sensitive personal data means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any court in such proceedings.

3 Purposes for sharing information

This Protocol covers information sharing for any purpose that supports the working of joined up services around an individual, unified service delivery, more effective service delivery across Partner Organisations (e.g. early intervention and prevention) and greater strategic insight across the borough.

3.1 Examples of sharing information

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.

Information sharing does not have to involve transfers of data. It could involve making information accessible or available, giving a professional or team access to systems for example.

3.2 Care purposes

3.2.1 Direct care

These purposes cover uses of data that contribute to the diagnosis, care and treatment of an individual or the audit of the quality of the care provided. With the exception of auditing, this can also be referred to as direct care. Where data are used for care purposes person identifiable data can be used providing that only the minimum necessary information is made available.

3.2.2 Non care

These purposes cover uses of data that support activities such as preventative medicine, medical research, financial management and the management of care services. Where data are used for non-care (or non-direct care) purposes, effectively anonymised or pseudonymised data must be used.

Broadly speaking direct care will be concerned with an individual, whilst non-direct care will involve large numbers of people, will involve individuals that are not known until after the data processing or will not involve contact with individuals.

4 Information sharing approaches

This Information Sharing Protocol provides a commitment by the signatories to ensure that a framework is in place that facilitates the sharing of information between Partner Organisations and respects the individual's right to privacy.

Information sharing requires commitment and advocates a proactive approach. By signing up, Partner Organisations are making a commitment to:

- show a willingness and commitment to sharing (appropriate information sharing will only occur when it is necessary, proportionate, relevant, accurate, timely and secure);
- ensure that there are clearly defined objectives for information sharing;
- facilitate the exchange of information where necessary to promote good quality and well-targeted public services;
- demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998 and other relevant legislation;
- adhere to the provisions laid out in this Protocol and to acknowledge their respective roles and responsibilities in implementing it;
- ensure that they and all relevant staff are aware of and comply with their responsibilities in relation to:
    - this Protocol;
    - information sharing agreements they enter into under it;
    - any procedures or guidance issued with regards to information sharing by their own organisation, Partner Organisations and national bodies; and
    - any legislation or regulation that they are subject to.
- promote public awareness of the need for information sharing through the use of appropriate communications media including publishing this Protocol on the websites of the respective agencies;
- share information within a framework where it supports the provision of better services to our service users and communities;
- ensure that information is shared safely and securely;
- ensure that in sharing information:
    - there is a clearly defined requirement;
    - it is lawful;
    - it accords with the Data Protection Act 1998;
    - only appropriate information is shared;
    - it is only available on a 'need to know' basis (i.e. the minimum information consistent with the purpose for sharing will be given);
    - it is only provided to those with a legitimate reason for access; and
    - it is in the interests of service users and communities.
- put in place governance that ensures that managers and staff are aware of their responsibilities as set out in this protocol and other data sharing

contracts related to it and recognise the need to work with Partner Organisations;

- work with Partner Organisations to develop guidance / tools (technical and non-technical) to support good information sharing;
- communicate the importance of appropriate information sharing to staff;
- ensure early consideration of information issues in service developments;
- be transparent with service users about how their personal data is going to be used, and respecting their privacy;
- ensure adherence to the ICO's Data Sharing Code of Practice;
- ensure that written information sharing agreements are developed and monitored for regular sharing of information and data;
- maintain a single register of information sharing agreements;
- work with Partner Organisations towards an aligned information policy framework to support safe and secure information sharing;
- ensure that the Caldicott principles are adhered to when sharing health information;
- put in place policies, procedures and controls (e.g. confidentiality, information security, data protection and records management) that ensure full compliance with the legal framework for sharing information;
- effectively notify the Information Commissioner's Office of the purposes for handling information under this protocol and maintain a valid data protection registration as appropriate;
- ensure that all information supplied is retained in line with any Records Management Policies, Codes of Practice and other legal requirements as relevant (e.g. when handling health data following NHS and Social Care Code of Practice);
- ensure that all personnel have access to appropriate training and development activities to enable them to comply with information sharing requirements;
- ensure that a complaints procedure, confidentiality policy and procedures, and risk assessment procedure are all in place, clearly linked to this protocol and adhered to;
- share depersonalised data where this would be more appropriate;
- ensure that all appropriate staff who have access to shared information have the necessary level of CRB clearance in accordance with relevant legislation;
- respond to any notices from the ICO or Court Orders that impose requirements to cease or change the way in which data is processed;
- ensure that appropriate resources are made available to enable and support sharing;
- use personal data disclosed to them under an agreement only for the specific purposes set out in the agreement (information disclosed will not be regarded

by that organisation as information for the general use of the organisation); and

- abide by any restrictions that may apply to any further use of non-personal data, such as commercial sensitivity or prejudice to others caused by the information released.

When sharing information, each signatory will commit to:

- ensuring that when acting as the Data Controller for information they will apply the conditions set out in the Information Sharing Agreement (ISA) and assume responsibility under the DPA.
- ensuring any new ISA will set out the purpose, use and scope of the data to be shared, the point at which responsibility moves from one Data Controller to another or the circumstances where the role of Data Controller is exercised together and the responsibilities of each agency signing this ISA
- ensuring that any new ISA will be specific and clearly identify only the data that needs to be shared.

5 Legal framework and guidance

The sharing of information may be governed by a number of different areas of law and guidance depending on whether it includes personal, personal sensitive or commercially sensitive data.

Before entering into any information sharing agreements all parties must consider the following:

- Consider whether the information can be anonymised or pseudo anonymised.
- Establish whether they have a power to carry out the function to which the information sharing relates.
- Check whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.
- Decide whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society.
- Decide whether the sharing of the data would breach any obligations of confidence.
- Decide whether the data sharing would be in accordance with the DPA, in particular the eight principles.
- Decide whether the data sharing would be in accordance with the Caldicott principles.
- If information to be shared could be made available under a Freedom of Information request, the organisation should consider proactively publishing the information on their website.

5.1 Data Protection Act

The conditions set out in Schedule 2 and 3 of the DPA are known as the “conditions for processing”. Organisations processing personal data need to be able to satisfy one or more of these conditions.

5.2 Basis for sharing

There are many factors that set out the basis for data sharing. For example:

- Section 47 of the NHS and Community Care Act 1990 provides for Social Services Authorities to involve staff of health and housing agencies in order to prepare comprehensive assessments of need. It can be implied from this duty that there is a power to share information with health bodies or housing authorities.
- Paragraph 16 of Schedule 2 to the NHS and Community Care Act 1990 provides that NHS Trusts have general powers to do anything which is necessary or expedient for the purposes of or in connection with the provision

of goods and services for the health service and similarly will give rise to an implied power to share information.

- Section 2 of the Local Government Act 2000 provides local authorities with powers to promote or improve the social wellbeing of their area. This provides an implied power to share information with other statutory services and the independent sector.
- Section 22 of the National Health Service Act 1977 provides for a general duty on NHS bodies and local authorities to cooperate with one another in order to secure and advance the health and welfare of the people of England and Wales. This general duty implies a power to share information between NHS bodies and local authorities.
- Section 115 of the Crime and Disorder Act provides a legal basis for sharing information between Community Safety Partnerships (CSP) partner agencies where it is necessary for fulfilling the duties contained in the Act.
- Under the Police and Justice Act, and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 made under the Act, when requested by a crime and disorder committee, responsible authorities and cooperating bodies are under a duty to share with the committee information that relates to the discharge of the authority's crime and disorder functions, or that relates to the discharge by the committee of its review and scrutiny functions under section 19 of the Police and Justice Act.
- Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Authorities are expected to support this by providing relevant information.
- Section 10 of the Children Act 2004 places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area. This statutory guidance for section 10 of the Act states good information sharing is key to successful collaborative working.

5.3 Duty of fairness

Under the DPA 1998 all Partner Organisations have a duty to:

- ensure they are open and transparent about their processes; and
- have in place, and issue to individuals where appropriate, the necessary Privacy Notices or Fair Processing Notices which clearly explain how information is shared, who it is shared with and for what reason.

It is a requirement of the DPA 1998 that all organisations that process personal data should have a "Fair Processing Notice" which will inform individuals about how their personal data will be used by the organisation to ensure that consent to the sharing

of personal information is informed. Partner Organisations agree to provide the following information to patients, clients or service users:

- the identity of the data controller and the Partner Organisations that work in partnership. If the data controller has nominated a representative for the purposes of the DPA 1998, the identity of the representative;
- the purpose or purposes for which the data are intended to be processed and shared;
- the rights of individuals under the DPA 1998, particularly in relation to sensitive personal data;
- details of the procedures in place to enable individuals to access their records, including audit trails, as regards access to data;
- details of the procedures which may have to be initiated when a member of Personnel suspects that an individual has been or is at risk of abuse for example under a 'Service User Protection Policy' or 'Mental Health Risk Assessment & Management Policy'. Such policies will explain in general terms to whom the personal information will be shared at differing stages, as well as what personal information will be shared, how it will be used and will be compliant with the Mental Capacity Act 2005;
- details of the complaints procedures to follow in the event that the individual concerned believes personal information about him or her has been inappropriately disclosed;
- Details of how the personal information individuals provide will be recorded, stored and the length of time it will be retained both by the originating organisation and the organisations to whom they may disclose that personal information;
- details of the length of time for which consent to particular disclosures is valid, for example in the case of adoption 75 years; and
- any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the individual to be fair.

Each party to this Agreement will ensure that the information referred to above will be made available to individuals in routine episodes of contact, assessment and care provision. All of the above notices will be referenced on each Party's website. The above information will be available in a variety of languages and formats where reasonable to reflect the ethnic composition across the borough.

5.4 Consent for sharing

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the conditions must be met whenever personal data is processed. Where possible individuals should be informed of and aware of the processing of their

information. Gaining consent (which is the first condition) is a mechanism for achieving both of these outcomes.

5.5 Consent for sharing information about care

Just having a basis for sharing is not enough to ensure sharing is fair and lawful. Consent (explicit consent for sensitive personal data) is one of the conditions in the DPA that can be met to legitimise processing or sharing information about care.

The NHS Constitution for England grants patients a right to privacy and confidentiality and to have their information treated safely and securely. In addition, the Social Care and NHS Care Records Guarantees for England specify that individuals are entitled to make their own decisions about how their confidential information is shared.

Whilst there may be circumstances to share information lawfully without obtaining an individual's consent, Health and Social Care Partner Organisations understand that individuals should be able to make decisions about what their information is used for and have their wishes respected as appropriate. When it comes to recording and sharing information all Health and Social Care Partner Organisations agree to the following:

- Each Partner Organisation, in its capacity as data controller, will be required to obtain consent from the individual.
- It will be the responsibility of the Partner Organisation that obtains the individual's consent to ensure that the individual's consent is valid, fully informed, express, explicit and reflects the true wishes of the individual as regards the sharing of data.
- Individual consent may be recorded in the respective records system of the Partner Organisation and should also be made available to Partner Organisations.

Where consent is being relied upon to legitimise the processing of information about care, Partner Organisations must ensure consent has been clearly documented ahead of any disclosure and maintained for a clear audit trail.

Consent should not be regarded as a permanent state. Consent needs to be gained for a specific data sharing activity and for a specific duration. Once the provision of this specific activity concludes or the purpose changes, then consent obtained for it will also end. Procedures must be in place to manage any consent withdrawals from individuals.

5.5.1 Sharing without consent

In some exceptional circumstances, personal information can be lawfully shared without consent where there is a legal requirement or where an appropriate professional of sufficient seniority within the Partner Organisation, has taken the view that the duty of confidentiality can be breached where there is a substantial over-

riding 'public interest'. Such situations where information might be shared without consent include:

- 'Life and death' situations, for example, where information is shared in an emergency in order to preserve life;
- where a person's condition indicates they may be a risk to the public or may inflict self-harm;
- in order to prevent abuse or serious harm to others; and
- on a case-by-case basis, to prevent serious crime and support detection, investigation and punishment of serious crime.

This is not an exhaustive list and each situation should be considered on a case by case basis.

Where decisions are made to share personal information without the person's consent, this must be fully documented in the person's record.

Where it is not appropriate to defer the sharing of information, then it will not be appropriate to defer consent, as consent cannot be obtained retrospectively. Therefore, only where deemed necessary, may personal information be shared without consent.

If there are any concerns relating to child or adult protection issues, practitioners must follow the relevant organisational procedures.

N.B. Where a statutory duty exists to share information and the sharing will happen regardless of the individual's wishes, consent should not be sought. Partner Organisations should instead seek to inform individuals of what sharing will happen and seek assurance that individuals understand this.

5.5.2 Obtaining consent where a person lacks mental capacity

The Mental Capacity Act 2005 Code of Practice defines the term 'a person who lacks capacity' as a person who lacks capacity to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken.

Whenever dealing with issues of capacity to consent, local rules and procedures should be followed and these must be in compliance with the Mental Capacity Act 2005 and its Code of Practice, and recorded on the consent agreement.

Where a person has a temporary loss of capacity consent will be deferred, if appropriate, until such time as consent can be obtained. Consent to share information will be sought when capacity is regained.

5.5.3 Refused and withdrawn consent

A person has the right to refuse their consent to have information about them shared. They also have the right to withdraw previously granted consent at any point,

to the sharing of their information. Further personal information should not then be shared.

Where the person has refused or withdrawn consent, the implications of withholding consent will be clearly explained to them. If a person withdraws consent to share personal information it will also be explained that information already shared cannot be recalled.

Where consent is refused or later withdrawn, this must be clearly recorded and monitored.

5.6 Duty of confidentiality

All Partner Organisations should be aware that they are subject to a Common Law Duty of Confidentiality, and must adhere to this.

“In Confidence” information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular were a professional relationship may exist (e.g. doctor/patient, social worker/client, lawyer/client).

The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised (i.e. it is not possible for anyone to link the information to a specific individual).

There are generally three categories of exception to the duty of confidence:

- where there is a legal compulsion to disclose;
- where there is an overriding duty to the public, or
- where the individual or organisation to whom the duty is owed has consented to disclosure.

The guidance from the Information Commissioner states that because such decisions to disclose 'in the public interest' involve the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions.

5.7 Control of information

Appropriate access procedures and controls must be agreed to limit the right to access the shared personal data to those who require it.

Where information is shared **with consent** of the individual, the data will be seen as being under the control of the party the information was shared with and they are responsible for any further sharing or use of it.

Where information is shared **without consent** of the individual, the information will be likely to remain under the control of the originating party. Further sharing not

consistent with the original sharing agreement should not take place without consultation with the originating party, or consent of the individual.

5.8 Subject access

Personal data must be processed in accordance with the rights of data subjects set out in the DPA 1998.

This includes the right of any individual to be provided access to any information held about them, whether in computer or manual files. This includes a right to be given details of the purposes for which their personal data is held, from whom it was obtained, and to whom it is or may be disclosed. This right, known as the right of subject access, is subject to a limited range of exemptions.

Partner Organisations must have appropriate procedures in place with regard to the handling of Subject Access Requests and staff must be appropriately trained in how to recognise and handle requests in line with legislation.

Unless statutory grounds exist for restricting an individual's access to personal information relating to him or her, an individual will be given every opportunity to gain access to personal information held about him or her and to correct any factual errors that have been made. Similarly, where an opinion about an individual has been recorded and the individual feels this opinion is based on incorrect factual personal information, the individual will be given every opportunity to correct the factual error and record his or her disagreement with the recorded opinion.

5.9 Data retention

Personal data should not be kept for longer than is necessary for the purpose or purposes for which is it processed.

Partner Organisations must ensure they have appropriate retention schedules in place which are adhered to along with any statutory requirements. Where no provision has been made best practice must be applied and the retention schedule updated accordingly to reflect best practice.

5.10 Records management

Officers carrying out the functions outlined in this ISP or supplementary ISAs should make themselves aware of, and adhere to, their organisation's records management procedures, specifically in relation to collecting, processing, retention and disclosing of personal information.

All information, whether held on paper or in electronic format must be stored and disposed of in line with each Partner Organisation's retention and disposal schedule.

Personal information will only be collected using the agreed collection methods, ensuring the required information is complete and up-to-date.

Officers will ensure where practical, that records are maintained of when information is shared with a Partner Organisation, and to whom.

Decisions about a person should never be made by referring to inaccurate, incomplete or out of date information.

If information is found to be inaccurate, officers will ensure that their records and systems are corrected accordingly. Consideration must also be given to advising Partner Organisations where practical.

Duplication of records will be avoided where practical and possible. Where a copy of information is required this should only be made in compliance with data protection guidance and law (e.g. DPA conditions), copies should be subject to the same data retention policy as the original and the copy should be updated when changes to the original are made.

6 Methodology for information sharing

This protocol can be taken as applicable to all forms of information sharing, irrespective of the method. In all situations and methods procedures should follow this protocol and any standards for best practice.

This agreement covers the following (non exhaustive) list of methods for information sharing in the first instance, each method must be supported by a detailed Information Sharing Agreement:

- Transfer of personal data to an Integrated Care IT System, shared record or to another record-holding system;
- Discussion in multi-disciplinary teams established for the purpose of delivering integrated care, support or assistance;
- Sharing of personal information for the purpose of crime prevention or investigation;
- Statutory reporting using anonymised data;
- Access to data by health and social care professionals in an MDT providing care to the patient/ service user; and
- Ad hoc reporting and data sharing for agreed purposes.

6.1 Procedures for data sharing

The following provides general guidance on different methods for sharing of personal data.

6.1.1 Transfer of information verbally (face to face)

Staff will ensure:

- the receiver of the information is properly identified
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- conversation cannot be overheard

6.1.2 Transfer of information by telephone/video conference

Transfer of information by telephone is not advised. Where it is unavoidable staff will ensure that:

- the recipient is properly identified and are sure they are talking to that recipient
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- conversation cannot be overheard
- a note of the conversation is logged

6.1.3 Transfer of information by fax

The use of fax transfer should be avoided whenever possible. Where it is unavoidable staff will ensure that they:

- use a “safe haven” fax machine
- phone the recipient to ensure that they are aware a confidential fax is about to be sent , send a fax covering sheet to confirm correct number, confirm that the individual will wait by the machine to collect the fax and notify the sender to confirm receipt.
- keep personal information to a minimum, by using a key identifier, i.e. NHS number, social services number or unique pupil number
- keep a log of confidential faxes sent and received

6.1.4 Transfer of information by post – internal or external

Printed information, or other media, containing **personal information** will only be sent by post or via courier:

- it will be opened by the addressee only
- envelope is sealed and marked “Personal & Confidential – to be opened by addressee only”
- full address details are used
- the addressee is informed the time, date and method that the information was sent and the addressee acknowledges receipt.
- Do not use internal envelopes

Printed information, or other media, containing **sensitive personal information** will only be sent via a secure channel. Secure channels include recorded or special delivery (where the letter/package can be tracked and signed for on delivery), or by using an approved courier service (the courier service should be approved for handling sensitive personal information).

6.1.5 Transfer of information by email

Email may be used for exchanging non personal (Level 1) information.

Email may be used to exchange non personal (Level 2) information if correctly managed. If using email to send non personal Level 2 data:

- ensure that exchanged information is adequately protected
- only send on a “need to know” basis
- ensure information is kept to a minimum
- ensure email system is protected by a password, which is kept secured
- Anonymise the information where possible

Email is not deemed a secure method for sending personal (Level 3) or sensitive personal (Level 3) information unless encryption (secure email) is used.

6.1.5.1 Secure email

Personal (Level 3) and sensitive personal (Level 3) data must only be shared by using secure email services. In this circumstance information must be sent from one secure email service directly to another (emails must not be copied or forwarded to non sensitive email services). The following is a list of secure email services:

.cjsm.net (Criminal and Justice)
.gcsx.gov.uk (Local Government/Social Services)
.gse.gov.uk (Central Government)
.gsi.gov.uk (Central Government including Department of Health)
.gsx.gov.uk (Central Government)
.hscic.gov.uk (The Health and Social Care Information Centre)
.mod.uk (Military)
.nhs.net (NHSmail)
.pnn.police.uk (Police)
.scn.gov.uk (Criminal and Justice)

6.1.5.2 Third party email encryption and secure file exchanges

Where the use of a secure email solution is not possible (e.g. where personal data must be sent to an organisation that does not have a secure email solution, such as a care home) then a third party email encryption or secure file exchange solution can be utilised.
Use of this third party solution is only possible if it is verified that the solution has a level of security appropriate to the type of data being sent and the same processes as used for sending standard email are followed (e.g. only send minimum data required, only send on a need to know basis).

6.2 Data quality

- Partner Organisations will have implemented or be working towards an Organisational Information Quality Strategy.
- Data quality needs to be of a standard fit for the purpose the information is to be used for, including being complete, relevant, reliable, valid, accurate and as up to date as required for the purposes for which it is being shared. The originating party must be able to evidence this and without this any decision made on the information may be flawed and inappropriate actions may result.
- Steps must be taken to validate information, such as checking with the person / party who originally provided the information, if staff are in any doubt as to its accuracy.
- Where practical and possible information should not be duplicated. Where data is duplicated it must be clear that the data is a duplicate and it must be maintained and updated
- If a data subject has informed a Partner Organisation that, in their view, the information is inaccurate, then a record should be made on the file that they

have expressed this view. Where such information has been shared with other Partner Organisations, they must be made aware of any actions taken in respect of inaccuracies or corrections made.

- If any member of staff records information either in writing or in an electronic format, the source of the information must also be clearly recorded as well as whether or not it is an opinion or factual observation.

6.3 Interoperability

Partner Organisations will bear in mind formatting and work towards ensuring that the data they share is compatible with the purposes of Partner Organisations. This will be done through considering the following issues when sharing information:

- Make sure that the format of the data being shared is compatible with the systems used by all involved organisations.
- System capability to use appropriate common identifiers to link data correctly.

6.4 Security

All Partner Organisations will maintain a safe haven to ensure the secure receipt and processing of personal data:

- Each Partner Organisation must have achieved or will be working towards a suitable level of information assurance (e.g. ISO 27001, IGT Level 2) or shown to be working towards a similar level of compatible security. Partner Organisations should ensure that the minimum standards of security that they require are agreed with Partner Organisations with whom their information will be shared and included in the information sharing agreement.
- Partner Organisations are to agree standard procedures to facilitate the exchange of information in a secure method reflective of the information being shared. Where a Partner Organisation has specific security requirements, for example a corporate policy, these policies should be made available to other Partner Organisations. This will assist in ensuring the agreed level of standards when entering into a new ISA.
- Any breaches of security, confidentiality and other violations of this ISP and subsequent ISAs must be reported in line with each Partner Organisation's incident reporting procedures. Consideration should be given to share, where appropriate, the outcome of any investigation with the Partner Organisations involved.

Where information is shared electronically the processes will conform to the following minimum standards:

- Role based access controls.
- Robust user authentication based on best practice.
- Network, hardware, database and application security controls.

- System monitoring and audit trails.
- System ability to generate alerts in the event of users by-passing access controls.
- System capability to respond to and deal with an individual's rights exercised under Part II of the DPA 1998.
- Protection of the confidentiality and integrity of data in transit including key management of cryptographic services to ensure the secure communication of data.
- Measures to safeguard against user error or system-to-system transfer errors by validating data input and transfer and ensuring inputs and transfers are correct and appropriate.
- All personal and sensitive personal data processed by the system will only be retained for as long as necessary.
- All personal and sensitive personal data processed by the system will be stored and destroyed securely.
- The system must contain appropriate intrusion detection and prevention controls to protect against unauthorised external access attempts.
- Appropriate controls to ensure the physical security of the system.
- Appropriate labelling of data (e.g. labelling of clinical data as "NHS Confidential").
- System capability to use appropriate common identifiers to link data correctly (e.g. NHS Number, National Insurance Number, DoB etc.).

6.4.1 Security of Information – Physical

Each Partner Organisation will ensure that the information is:

- physically protected from potential damage arising from environmental hazards such as fire and flood.
- held on premises that are adequately protected from unauthorised entry and / or theft or destruction.

6.4.2 Security of information – IT systems

Each Partner Organisation will:

- comply with any relevant policy or guidance on IT systems and security
- only hold the information on secure servers, not on portable media or devices such as laptops or USB memory sticks or CD-ROMs or employees' own personal computers, unless appropriately encrypted.
- ensure adequate back-up facilities to minimise the risk of loss of or damage to the information and that a robust business continuity plan is in place in the event of restriction of service for any reason.
- transmit the information by use of the approved method as described above.

- commit to minimising paper and only make printed paper copies of the information if this is essential for delivery of the service. Any printed paper copies of the information must be stored in a locked cabinet within a secure office when not in use.

6.4.3 Security of Information – Employees

Each Partner Organisation will:

- undertake all pre-employment checks to verify the identity, honesty, trustworthiness and general suitability of employees (including CRB checks where appropriate).
- include appropriate confidentiality clauses in employment contracts, including details of sanctions against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of DPA 1998 or causes damage to or loss of the information.
- ensure that their own employees and individuals working on their behalf, including bank staff, temporary workers or contractors are aware of and act in accordance with relevant policies and legal requirements, and are adequately trained to understand and comply with their responsibilities under this ISP and subsequent ISAs.

6.5 Overseas transfers

In accordance with the Data Protection Act personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Where it is necessary to transfer data outside of the EEA the transfer can only take place after approval by all involved Partner Organisations

6.6 Data Transparency

This Protocol commits Partner Organisations to being proactive in publishing non-sensitive information. Partner Organisations should understand what they hold, what their communities want and then release it in a way that allows the public, developers or the media to use it.

Under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) organisations may be obliged to publicly disclose information on their records. This may include information a Partner Organisation has received under an agreement made pursuant to this Protocol.

It is for the Partner Organisation in receipt of a request under the FOIA to decide how it responds, including deciding whether any of the exemptions to disclosure apply. In reaching this decision Partner Organisations may need to consult affected

third parties, including the other Partner Organisations signed up to this Protocol, for their views on the request.

When deciding whether it is necessary to consult third parties, Partner Organisations should be guided by the code of practice issued under section 45 of the FOIA. Whilst views of third parties should be taken into account, it is ultimately for the organisation in receipt of a request to decide how it shall respond.

The FOIA requires public sector organisations to operate a publication scheme approved by the Information Commissioner's Office that sets out information that must be routinely published. Public sector organisations should also work towards maintaining an inventory of the information they hold. If public data would be released under Freedom of Information it should be included in the inventory.

6.7 Auditing of the system

Notwithstanding that each organisation will have its own audit procedures and programme in place all parties agree to allow the external auditors of any other party involved in sharing data permission to audit the other parties' implementation of the system to ensure compliance with this ISP and any subsequent ISAs. Such permission shall not be unreasonably withheld.

7 Governance

7.1 Notification with the Information Commissioners Office (ICO)

The DPA 1998 requires all data controllers who process personal data to make a formal notification of its processing to the Information Commissioner. They must inform of the purposes for handling information under this Protocol and maintain a valid data protection registration as appropriate. It is particularly important when engaging in information sharing that the purposes for which the data are to be used are included in the notification.

7.2 Information Management Group

Each Partner Organisation will nominate an Information Management Group / Group of Senior Officers as appropriate that will be responsible for managing the information exchanges within their organisation. Each group will:

- ensure that their organisation has an up-to-date and accurate data protection notification (registered with the Information Commissioner) which allows for the collection, use and transfer of the data to be shared;
- develop systems of implementation, dissemination, guidance, training and monitoring to ensure that this framework is known, understood and followed by all employees and contractors who need to share information;
- promote good practice in the sharing of personal data by ensuring compliance with the principles, purposes and processes of this framework;
- be responsible for agreeing and signing information sharing agreements under this Protocol;
- maintain a register of information sharing agreements made under this Protocol; and
- make available to Partner Organisations as required the names and contact details of the officers who sit on the group.

7.3 Employees

It should be recognised that Information Sharing may come into anyone's role. All staff will recognise the importance of and undertake responsibility for facilitating this.

Each Partner Organisation must ensure:

- that all personnel have access to appropriate training and development activities to enable them to comply with information sharing requirements. They must have an appropriate level of knowledge of the contents of this Protocol, plus any additional requirements of their own organisation, to take responsibility for agreeing such disclosures.

Every employee working for or on behalf of a Partner Organisation:

- is personally responsible for the safekeeping of information they obtain, hold, use or disclose in the course of their job;
- should have a suitable level of awareness and training in how to obtain, use and share information appropriately; and
- must, before disclosing information under this Protocol or any agreements under it, take any necessary steps to ascertain the identity and authority of any intended recipient of that information.

7.4 Caldicott Guardian

All NHS and Social Care organisations **must** appoint a Caldicott Guardian who will act as the 'gatekeeper' of service users' care information.

All Partner Organisations recognise the requirements that Caldicott imposes on NHS organisations and social services departments. They will ensure requests for information from these organisations are dealt with in a manner compatible with these requirements.

7.5 Data Protection Incidents

Each Partner Organisation must have a current, agreed and published policy on handling Data Protection Incidents.

Data Protection Incidents must be handled in line with the corporate policy of the organisation where a breach has occurred in accordance with the Information Commissioner's "Guidance on data security breach management". The Partner Organisation who discovers the breach must inform the relevant Partner Organisations immediately where appropriate, giving full details of the nature and extent of the breach.

In dealing with the breach or suspected breach the party that is the 'Information Owner' will implement any steps necessary to rectify the breach and mitigate future incidents any other parties will co-operate as far as is legally possible.

7.6 Complaints

All Partner Organisations must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal data, received from both staff and members of the public.

The Partner Organisations confirm to each other that:

- they have put in place efficient and effective procedures to address complaints relating to the disclosure of personal information, and data subjects will be provided with information about these procedures where it is deemed relevant;
- they will keep a record of all such complaints received; and
- they have established a procedure by which their complaints officers report complaints regarding the inappropriate use or disclosure of personal

information to the Caldicott Guardian or Information Governance Lead / Data Protection Officer or equivalent.

8 Monitoring & Review

All Partner Organisations must ensure that a complaints procedure, confidentiality policy and procedures, and risk assessment procedure are all in place, clearly linked to this Protocol and adhered to.

It is important to also monitor and understand information flows between and within organisations to enable Partner Organisations to identify which information has the most value, and when to review and improve practices.

Organisations should also monitor the flow of information in order to mitigate the risk of data breaches, and should be capable of documenting a clear audit trail to evidence this.

8.1 Management of the Protocol

The organisations that are signatories to a protocol have responsibility for:

- Ownership of the Protocol
- Approving the content of the Protocol
- Ensuring dissemination of the Protocol
- Agreeing and arranging training as required on the Protocol
- Implementing the requirements of the Protocol within their organisation
- Monitoring implementation and compliance of the Protocol
- Reviewing and recommending any changes to the Protocol.

8.2 Reviewing the Protocol

It is envisaged that this Protocol will evolve, especially as new Partner Organisations join. The Protocol will be subject to a formal review process annually to be instigated and managed by the responsible Information Management Group/function.

Any changes to the contents will be formally approved and adopted following consultation and agreement with signatories of the Protocol.

All staff responsible for information sharing under this Protocol will be informed of any changes. Training (where necessary) will be undertaken. All documentation will be amended and version controlled.

8.3 Monitoring of Individual Sharing Agreements

All Partner Organisations must implement and communicate a procedure for monitoring individual Sharing Agreements. Periodic reviews must be undertaken to assess whether the stated objectives have been determined etc. The individual Sharing Agreements should be amended and agreed to reflect any changes required following the review.

Partner Organisations must identify and log incidents in relation to individual Sharing Agreements which highlight any non-compliance.

The following incidents will be logged and reported:

- Refusal to disclose information and reasons for refusal
- Additional conditions being placed on disclosure
- Delays in responding to requests for information (FOI and SAR)
- Disclosure of information to members of staff who do not have a legitimate "need to know"
- Inappropriate or inadequate use of the procedures
- Disregard of the Protocol and agreed security procedures
- Use or disclosure of personal data for purposes other than those agreed in the specific Information Sharing Agreement
- In the case of shared databases, actual or suspected breach

Non-compliance by a Partner Organisation will be reported to that organisation's data protection officer. Instances of a DPA incident must be dealt with promptly and in line with ICO guidance. Additional details of how breaches will be handled should be provided in the specific Information Sharing Agreement.

9 Undertaking / Agreement

The signatories to the Protocol agree to accept the procedures laid down in this protocol and are committed to providing a secure framework for sharing personal data between their agencies in a manner compliant with their statutory and professional responsibilities.

10Signatories

Authority / Organisation being represented	Name of Responsible Officer and role	Signature	Date

11Appendix A: Associated Legislation

11.1 Data Protection Act

(http://www.legislation.gov.uk/ukpga/1998/29/contents)

The key piece of legislation governing the collection and use of personal data is the **Data Protection Act 1998** (the DPA).

The term "personal data" is defined in the DPA as:

- 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.

The DPA both:

- grants rights to individuals (data subjects) in respect of their personal data and
- obliges those that process (e.g. collect, hold and use) personal data to do so in accordance with a set of data protection principles contained within the Act.

11.1.1 Rights of individuals

The DPA gives seven rights to individuals in respect of their personal data held by others. They are:

1. The right of subject access
2. The right to prevent processing likely to cause unwarranted substantial damage or distress
3. The right to prevent processing for the purpose of direct marketing
4. Rights in relation to automated decision taking
5. The right to take action for compensation if the individual suffers damage
6. The right to take action to rectify, block, erase or destroy inaccurate data
7. The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the DPA has been contravened.

11.1.2 Data Protection principles

The use of personal data is regulated by eight Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
   a. at least one of the conditions in Schedule 2 is met, and

   b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or purposes.
6. Personal data shall be processed in accordance with the rights of Data Subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

11.1.3 Schedule 2 (first data protection principle)

The first data protection principle requires that at least one of the conditions in Schedule 2 of the DPA be met before personal data can be processed fairly and lawfully. These conditions are:

1. The Data Subject has given their consent to the processing
2. The processing is necessary
   a. for the performance of a contract to which the Data Subject is a party, or
   b. for the taking of steps at the request of the Data Subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract
4. The processing is necessary in order to protect the vital interests of the Data Subject
5. The processing is necessary
   a. for the administration of justice
   b. for the exercise of any functions conferred on any person by or under any enactment
   c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

6. The processing is necessary for the purposes of “legitimate interests” pursued by the Data Controller or by the third party or parties to whom the data are disclosed.

When applying condition (6) you must further ensure that once you have established that there is a legitimate interest, these interests must be balanced against the interests of the individual(s) concerned. The “legitimate interests” condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual’s legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

11.1.4 Schedule 3 (first data protection principle)

When processing “sensitive personal data” the first data protection principle requires that at least one of the conditions in Schedule 3 of the DPA be met in addition to a Schedule 2 condition.

The conditions in Schedule 3 DPA are:

- The Data Subject has given their “explicit” consent to the processing
- The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment
- The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another
- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject
- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice
- The processing is necessary for the administration of justice or carrying out legal or public functions

11.2 The Human Rights Act 1998

(http://www.legislation.gov.uk/ukpga/1998/42/contents)

The Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public

authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

Article 8 of the Act states: "Everyone has the right to respect for his private and family life, his home and his correspondence..."

The Act further states that this is not an absolute right and acknowledges that under certain conditions this right can be lawfully overridden. The following considerations should be made: -

- Is there a legal basis for the action being taken?
- Does the action pursue a legitimate aim?
- Is the action being taken proportionate and undertaken in the least intrusive manner?

11.3 Caldicott Principles

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

The Caldicott Principles apply to organisations dealing with personal data in relation to health and social care. These organisations are required to observe the following principles when using personal information and assign a senior officer to the role of Caldicott Guardian for the organisation:

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.
2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal 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).
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.
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 mean introducing access controls or splitting data flows where one data flow is used for several purposes.
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.

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.
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.

11.4 Common Law Duty of Confidentiality

(http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173)

Common law is not specifically written out in one document, but is applied by reference to previous cases, common law is more a requirement based on precedent.

“In Confidence” information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has been informed and consented;
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest; or
- where there is a legal duty to do so, for example a court order.

Where a disclosure is in the public interest a solid justification is required before individual rights are set aside before the information is disclosed. Any decision to disclose should be fully documented.

The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

11.5 Freedom of Information Act 2000

(http://www.legislation.gov.uk/ukpga/2000/36/contents)

Public Sector bodies are encouraged to be open and transparent in providing information to the public. Publication of 'level 1' data (as defined in section 2) wherever possible is a mechanism to assist in meeting our commitment. Our Partner Organisations are encouraged to use a similar approach where possible

Under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) Partner Organisations may be obliged to publicly disclose information on their records. This may include information a Partner Organisation has received under an agreement made pursuant to this Protocol.

There are 23 statutory exemptions to the right of access which are either absolute or qualified. Absolute exemptions include the release of personal data where it would breach the Data Protection Act. Qualified exemptions require the undertaking of a public interest test to consider whether the exemption will apply.

It is for the Partner Organisation in receipt of a request under the FOIA to decide how it responds, including deciding whether any of the exemptions to disclosure apply. In reaching this decision Partner Organisations may need to consult affected third parties, including the other Partner Organisations signed up to this protocol, for their views on the request.

When deciding whether it is necessary to consult third parties, Partner Organisations will be guided by the code of practice issued under section 45 of the FOIA. Whilst views of third parties should be taken into account, it is ultimately for the Partner Organisation in receipt of a request to decide how it shall respond.

The Code of Recommended Practice for Local Authorities for Data Transparency requires the council, and Partner Organisations, to understand what they hold, what their communities want and then release it in a way that allows the public, developers or the media to use.

The FOIA requires local authorities to operate a publication scheme approved by the Information Commissioner's Office that sets out information that must be routinely published. Partner Organisations will need to provide information for the purposes of complying with the requirements of the publication scheme.

Partner Organisations should build and maintain an inventory of the public data that they hold so that people are able to know what is available to them. If public data would be released under Freedom of Information it should be included in the inventory. Partner organisations may need to contribute to the inventory list compiled by the council.

11.6 The Access to Health Records Act 1990 ("AHRA")

(http://www.legislation.gov.uk/ukpga/1990/23/contents)

The DPA 1998 supersedes the AHRA apart from the sections dealing with access to information about the deceased. The AHRA provides rights of access to health records of deceased individuals for their personal representatives and others having

a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should be carried out in such a way as to comply with the common law duty of confidentiality.

11.7 NHS Health Service Act 2006

(http://www.legislation.gov.uk/ukpga/2006/41/contents)

Section 251 of the NHS HSA gives the Secretary of State the power to make regulations relating to the processing of prescribed patient information for medical purposes in the interests of patients or the wider public good (e.g. disclosing patient identifiable information to specified bodies, such as cancer registries).

The proposed use of patient identifiable information for which regulations under Section 251 are made must be acceptable under the HSA. Acceptable purposes are preventative medicine, medical diagnosis, medical research, provision of care and treatment, management of health and social care services and informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care or treatment but the primary purpose of the processing cannot be to determine the care and treatment of specific patients.

Section 251does not change the DPA 1998 requirements but where regulations apply it does set aside the legal duty of confidentiality and replace it with a range of safeguards intended to ensure that the use of a patient's information has no detrimental effect on that patient. The existing regulations under Section 251 are in the Health Service (Control of Patient Information) Regulations 2002.

11.8 The Health and Social Care Act 2012

(http://www.legislation.gov.uk/ukpga/2012/7/contents)

The HSCA reshapes the structure of the NHS. It transfers commissioning powers to new organisations, CCGs and NHS England. Importantly, the HSCA empowers the Health and Social Care Information Centre to process health and social care patient confidential information.

11.9 The ISO/IEC 27000 Series on Information Security Standards

(http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)

This Standard provides a code of practice and a set of requirements for the management of information security. The Standard is published in two parts. Part 1 provides a code of practice for information security management. Part 2 provides recommendations and controls for information security management systems.

11.10 NHS Care Record Guarantee

(http://systems.hscic.gov.uk/rasmartcards/strategy/nhscrg)

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over

this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records. Whilst not a legal document, the Guarantee could be used as the basis for a complaint.

11.11 Social Care Record Guarantee

(http://webarchive.nationalarchives.gov.uk/20130513181011/http://www.nigb.nhs.uk/pubs/screngland)

The Social Care Record Guarantee for England sets out the rules that govern how service user information is used within both Adults and Children's Social Care Services and what control individuals can have over this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records. Whilst not a legal document, the Guarantee could be used as the basis for a complaint.

11.12 The Information Security NHS Code of Practice

(https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice)

The Information Security Code of Practice has been published by the Department of Health and provides a guide to the methods and required standards of practice in the management of information security in the NHS.

11.13 The Records Management NHS Code of Practice

(https://www.gov.uk/government/publications/records-management-nhs-code-of-practice)

The Code offers detailed guidance on the management of all NHS record types, clinical and corporate records and provides minimum retention period schedules for NHS records.

11.14 The NHS Code of Practice

(https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)

This code of practice sets out standards to ensure that patient information is handled fairly, lawfully and as transparently as possible.

11.15 The Information Commissioner's Office Data Sharing Code of Practice

(https://ico.org.uk/media/about-the-ico/consultations/2069/data_sharing_code_of_practice.pdf)

This code explains how the Data Protection Act 1998 (DPA) applies to the sharing of personal data. It also provides good practice advice that will be relevant to all organisations that share personal data. The code covers activities such as:

- a group of retailers exchanging information about former employees who were dismissed for stealing;
- a local authority disclosing personal data about its employees to an anti-fraud body;
- a primary school passing details about a child showing signs of harm to the police or a social services department;
- the police passing information about the victim of a crime to a counselling charity;
- a GP sending information about a patient to a local hospital;
- the police and immigration authorities exchanging information about individuals thought to be involved in serious crime;
- a supermarket giving information about a customer's purchases to the police;
- two departments of a local authority exchanging information to promote one of the authority's services;
- two neighbouring health authorities sharing information about their employees for fraud prevention purposes;
- a school providing information about pupils to a research organisation; and
- a retailer providing customer details to a payment processing company

11.16 The National Archives Records Management Code

(http://www.nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/)

The National Archives is working to promote compliance with the Code of Practice on the management of records in all public authorities.

11.17 Ministry of Justice FOI Code of Practice

(http://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/code-of-practice)

This code of practice, issued under section 45 of the Freedom of Information Act, sets out the practices which public authorities should follow when dealing with requests for information under the Act. It provides clear guidance on providing advice and assistance to applicants, transferring requests to other authorities, consulting third parties, the use of confidentiality clauses in contracts and the provision of internal complaints procedures

12Appendix B: Example Statutory Gateways

There are a number of legal gateways that will allow the sharing and disclosure of personal information. Listed below are merely a few of the more commonly used ones. It is the responsibility of each organisation to ensure they have identified an appropriate legal gateway before sharing any personal information.

12.1 Crime and Disorder Act 1998

(http://www.legislation.gov.uk/ukpga/1998/37/contents)

The Act introduced measures to reduce crime and disorder. Section 115 provides that any person has the power to lawfully disclose information to the police, local authority, probation service or health authority (or persons acting on their behalf) where they do not otherwise have the power, but only where the disclosure is necessary or expedient for the purposes of any provision of the Act.

However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information and does not override the need to disclose in a proper manner taking into account Data Protection Principles and Article 8 Human Rights Convention.

12.2 Local Government Act 2000

(http://www.legislation.gov.uk/ukpga/2000/22/contents)

Under Section 2 local authorities may do anything, which they consider likely to achieve any one or more of the following objectives:

- the promotion or improvement of the economic well-being in their area;
- the promotion or improvement of the social well-being of their area; and
- the promotion or improvement of the environmental well-being of their area.

The power may not be exercised where there is an express restriction on doing so.

12.3 National Health Service and Community Care Act 1990

(http://www.legislation.gov.uk/ukpga/1990/19/contents)

Under Section 47 when a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the appropriate primary care trust or local housing authority and invite them to assist to such extent as is reasonable in the circumstances in the making of the assessment.

12.4 Children Act 1989

(http://www.legislation.gov.uk/ukpga/1989/41/contents)

Sections 27 and 47 of the Children Act 1989 enable local authorities to request help from specified authorities (other local authorities, education authorities, housing authorities, NHS bodies) and place an obligation on those authorities to co-operate.

A request could be for information in connection with a section 17 needs assessment or a section 47 child protection enquiry.

12.5 Children Act 2004

(http://www.legislation.gov.uk/ukpga/2004/31/contents)

The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children.

Section 10 (co-operation to improve well-being) establishes a duty on local authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key Partner Organisations to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.

Section 11 (arrangements to safeguard and promote welfare) brings with it an implied duty to share information when judged to be in the best interests of the child. That is, those bodies bound by the duties should share information about children as part of furthering those duties. The Children Act 2004, therefore, adds to and reinforces the existing body of legislation that gives (usually in an implied way) legal foundation to information sharing when the interests of a child require it.

12.6 Education Act 2002

(http://www.legislation.gov.uk/ukpga/2002/32/contents)

S175 (2) provides that the governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.

12.7 Mental Capacity Act 2005

(http://www.legislation.gov.uk/ukpga/2005/9/contents)

The Mental Capacity Act 2005 covers people in England and Wales who can't make some or all decisions for themselves. The ability to understand and make a decision when it needs to be made is called 'mental capacity'.

12.8 National Health Services Act 1977

(http://www.legislation.gov.uk/ukpga/1977/49/introduction)

12.9 The Environmental Information Regulations 2004

(http://www.legislation.gov.uk/uksi/2004/3391/contents/made)

Public authorities have a legal obligation to provide information about the environment through an approved publication scheme and in response to requests

13Appendix C: Consent

13.1 What is meant by "consent"?

One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question. You will need to examine the circumstances of each case to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a customer's failure to return a form or respond to a leaflet.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if your organisation intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, you should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which you are collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

You should review whether a consent you have been given remains adequate as your organisation's relationship with an individual develops, or as the individual's circumstances change.

Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

As explained above, a particular consent may not be adequate to satisfy the condition for processing (especially if the individual might have had no real choice about giving it), and even a valid consent may be withdrawn in some circumstances. For these reasons an organisation should not rely exclusively on consent to legitimise its processing. In our view it is better to concentrate on making sure that you treat individuals fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.

Extracted from the Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/)

13.2 Obtaining consent

The approach to obtaining consent should be transparent and respect the rights of the person.

Consent is where the person actively agrees, to a particular use or disclosure of personal information. It can be expressed either verbally or in writing, although written consent is preferable since that reduces the scope for subsequent dispute.

Consent must not be secured through coercion or inferred from a lack of response to a request for consent. Practitioners must be satisfied that the person has understood the information sharing arrangements and the consequences of providing or withholding consent.

When dealing with sensitive personal information consent must be explicit (Schedule 3 of the DPA 1998). There is no clear definition of what 'explicit consent' means. But the Information Commissioner's guidance says that the consent must be absolutely clear: it should cover the specific processing details, the type of information (or even the specific information), the purposes of the processing, and any special aspects that may affect the individual, such as any disclosures that may be made.

Where the person is a child or young person, the practitioner should consider whether the child or young person has the capacity to understand the implications of giving their consent in the particular circumstance. Where the practitioner is confident that the child or young person can understand their rights, then consent should be sought from them rather than a parent. It is important that a child or young person is able to understand (in broad terms) what it means to give their consent.

Where the person has a lack of mental capacity to understand the implications of sharing, their lawful representative will act on their behalf.

14 Appendix D: Information relating to minors and young persons

Recent legal precedents have changed the interpretation of the law relating to releasing information about minors and young persons. The following summarises these changes:

A person will need to present legally acceptable evidence that they have parental responsibility (e.g. a Residence Order).

Someone with parental responsibilities can submit a data subject access request on behalf of a child. However, if the child is at an understandable age (not defined under the Data Protection Act, but best practice is to consider whether the child is Gillick competent) then the child must give consent to the person with parental responsibilities for them to access the information on their behalf.

The organisation will abide by the Department of Health Reference Guide to Consent for Examination or Treatment (August 2009) in assessing whether a child is 'Gillick competent' or whether they meet the 'Fraser guidelines'. For more information please reference: http://www.nspcc.org.uk/Inform/research/briefings/gillick_wda101615.html

15Appendix E: Useful links

The government data standards catalogue	http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif/datastandards.aspx
For local government	http://standards.esd.org.uk
For the NHS and Social Care	http://www.hscic.gov.uk/
The Information Commissioner's Office (ICO)	http://ico.org.uk/
The ICO Data Sharing Code of Practice	http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing
Mental Capacity Act 2005 Code of Practice	https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice
The ICO guidance on Privacy Notices	http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices
Ministry of Justice Guidance on the law of Public Sector data sharing	http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf

Home Office - Information sharing for community safety	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97842/guidance.pdf
ICO guidance on exemptions from the Data Protection Act	https://ico.org.uk/for_organisations/data_protection/the_guide/exemptions
Mandatory minimum requirements for protection of personal data	http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-e-mandatory-minimum-measures.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60968/cross-gov-actions.pdf

16Document History

Date	Version	Author	Comment
22/10/14	0.1	Ian Bacchus	Initial draft
03/11/14	0.2	Ian Bacchus	Updated following first internal review
05/11/14	0.3	Ian Bacchus	Reviewed before project team review
10/11/14	0.4	Ian Bacchus	Updated to support ISA Template
02/12/14	0.5	Ian Bacchus/Lucy Martin	Updated to reflect wider coverage and use for the protocol
02/02/15	0.6	Ian Bacchus/Lucy Martin	Further updates (mostly grammatical) to support wider use Inclusion of feedback from IG Working Group review
03/02/15	1.0	Ian Bacchus	Final version for sign off