Information Sharing Policy

Controlled document
This document is uncontrolled when downloaded or printed.

<table>
<thead>
<tr>
<th>Reference number</th>
<th>WHHT: IT010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Author Name &amp; Job Title</td>
<td>Nicola Bateman, Information Governance Manager</td>
</tr>
<tr>
<td>Executive Lead</td>
<td>Lisa Emery</td>
</tr>
<tr>
<td>Approved by date</td>
<td>Jan 2016</td>
</tr>
<tr>
<td>Ratified by</td>
<td>Informatics Group</td>
</tr>
<tr>
<td>Committee/individual responsible</td>
<td>Informatics Group</td>
</tr>
<tr>
<td>Issue date</td>
<td>January 2016</td>
</tr>
<tr>
<td>Review date</td>
<td>January 2018</td>
</tr>
<tr>
<td>Target audience</td>
<td>All WHHTUK Staff</td>
</tr>
<tr>
<td>Additional Search Terms (Key Words)</td>
<td>Information Sharing Agreements</td>
</tr>
<tr>
<td>Previous Policy Name</td>
<td>n/a</td>
</tr>
</tbody>
</table>
CONTRIBUTION LIST

Key individuals involved in developing this version of the document

<table>
<thead>
<tr>
<th>Name</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nicola Bateman</td>
<td>Information Governance Manager</td>
</tr>
<tr>
<td>Michael Van de Watt</td>
<td>Caldicott Guardian</td>
</tr>
<tr>
<td>Lisa Emery</td>
<td>Senior Information Risk Owner</td>
</tr>
</tbody>
</table>

Approved by Committee | Informatics Group

CHANGE HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Jan 2016</td>
<td>Nicola Bateman</td>
<td>New Policy required for Information Governance requirements</td>
</tr>
</tbody>
</table>
Table of Contents

CHANGE HISTORY ........................................................................................................................................... 2

1. INTRODUCTION ........................................................................................................................................ 4

2. PURPOSE ..................................................................................................................................................... 4

3. RESPONSIBILITIES ...................................................................................................................................... 5

4. INFORMATION GOVERNANCE TOOLKIT (IGT) ....................................................................................... 6

5. INFORMATION SHARING PARTNERS ......................................................................................................... 6

6. INFORMATION SHARING AGREEMENTS (ISA) ....................................................................................... 7

7. PURPOSES FOR SHARING INFORMATION ............................................................................................ 7

8. WHEN IS AN ISA REQUIRED? ................................................................................................................ 8

9. FACTORS TO CONSIDER BEFORE SHARING ..................................................................................... 9

10. PRIVACY IMPACT ASSESSMENTS .......................................................................................................... 10

11. A SUMMARY OF LEGAL & NHS MANDATED FRAMEWORKS FOR SHARING INFORMATION ........... 10

12. THE DATA PROTECTION ACT 1998 ....................................................................................................... 10

   12.1. Fair and Lawful Processing ............................................................................................................... 11

   12.2. Schedule 2 Conditions ..................................................................................................................... 12

   12.3. Schedule 3 Conditions ..................................................................................................................... 14

13. THE HUMAN RIGHTS ACT 1998 & EUROPEAN CONVENTION OF HUMAN RIGHTS .................. 17

14. COMMON LAW DUTY OF CONFIDENCE ............................................................................................. 18

   14.1. Consent ............................................................................................................................................... 18

   14.2. Public Interest .................................................................................................................................... 19

   14.3. Statutory Gateways .......................................................................................................................... 21

15. LEGISLATION THAT IMPACTS ON THE NHS .................................................................................... 22

16. MONITORING & AUDIT .......................................................................................................................... 22

17. REFERENCES .............................................................................................................................................. 23
1. Introduction

West Hertfordshire Hospitals NHS Trust has a legal responsibility to ensure personal information is lawfully obtained, properly controlled and that an individual’s autonomy is respected. It is important to achieve a balance between the need to share information in order to provide quality care and respecting the privacy of patients by keeping information confidential.

The legal framework for information sharing is complex and there are legal and professional obligations that limit, prohibit or set conditions in respect of the use and disclosure of personal information and, similarly, statutes that permit or require information to be used or disclosed.

Recently, the Health and Social Care (Safety and Quality) Act 2015 introduced a new legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. The new Act reinforces existing good practice and obligations on health and social care professionals and provides statutory support for the seventh Caldicott principle that – “the duty to share information can be as important as the duty to protect confidentiality”. It makes it clear that unless an individual objects, then information can be lawfully shared between health and social care providers for purposes to facilitate the provision of health services and social care in an individual’s best interests.

This policy summarises the legal framework within which public sector data sharing can take place. The policy also explains the key principles which will facilitate the sharing of personal data between partner organisations and when information is required for either direct health care purposes or for other non-medical purposes, as required by legislation or statutory gateways.

2. Purpose

The purpose of this policy is to:

- clarify the legal background on information sharing
- provide assurance to the Trust Board that the Trust has a managed information sharing process in place.
- facilitate the secure sharing of information amongst key public sector, private and voluntary organisations across organisational boundaries
- define the framework within which the Trust can develop Information Sharing Agreements (ISAs) for specific areas of service.
- promote staff awareness of the legal framework for information sharing, the obligations on the Trust to protect personal information, and the standards and procedures for appropriate information sharing.
- ensure the Trust meets its statutory obligations with regard to sharing personal information.
This policy will be underpinned by established Information Sharing Agreements between the Trust and our information sharing partners.

3. Responsibilities

The Chief Executive Officer is the Accounting Officer of the Trust and has overall accountability and responsibility for Information Governance.

The Senior Information Risk Owner (SIRO) will oversee the development of the Information Risk Management Policy and take ownership of the risk assessment process for information risk.

The Caldicott Guardian will act as the ‘guardian’ of patient identifiable information and will oversee the use and sharing of patient information.

The Information Governance Manager will manage the day to day Information Governance agenda, including embedding appropriate Information Sharing Agreements between the Trust and all Third Party Providers and Data Processors that receive personal identifiable information.

Information Asset Owners (IAO) are senior individuals and are directly accountable to the SIRO. The IAO role is to:

- understand the nature and justification of information flows to and from their information asset
- ensure the confidentiality, integrity, and availability of all information that their system processes
- know who has access to the asset and why, whether it be to the system application or it’s information contents to ensure access is monitored and compliant with policy
- understand and address risks to the information assets they own
- provide assurance to the SIRO on the security and use of assets

Information Asset Administrators (IAA) provides support to their IAO. To do this they will:

- ensure policies and procedures are followed
- recognise potential or actual security incidents
- consult their IAO on incident management

Senior Managers are responsible for completing the annual data mapping returns, ensuring all outbound and inbound data flows are identified and mapped including the details of all third party providers that receive personal identified information.
All staff will have a responsibility to comply with legislation and guidance relating to information sharing and identify and report any risks, non-compliance or areas of concern.

4. Information Governance Toolkit (IGT)

The IG Toolkit is a Department of Health (DH) online system that the Health and Social Care Information Centre (HSCIC) is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in a single standard as a set of information governance requirements.

All organisations that have access to NHS patient data must provide assurances that they are practising good information governance and use the IG Toolkit to evidence this by way of annual self assessments.

The purpose of the assessment is to enable organisations to measure their compliance against these requirements to ensure information is handled correctly and protected from unauthorised access, loss, damage and destruction.

The ultimate aim is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information. This, in turn, increases public confidence that the NHS and its partners can be trusted with personal data.

5. Information Sharing Partners

Information sharing partners will cover a range of organisational types, some of which will be ‘trusted’ organisations, whilst others will not. Organisations that can demonstrate they are attaining an acceptable level of information governance performance are those that are meeting level 2 attainment or above on all requirements.

The following organisations are mandated to undertake annual information governance assessments and ensure they reach an acceptable standard:

- NHS organisations, including foundation trusts and NHS commissioners;
- Local authority public health teams;
- Clinical Commissioning Groups (CCG) & Commissioning Support Units (CSU)

Other organisations have a requirement to meet the key requirements because they are working with or for NHS organisations, are processing NHS patient information or have access to national NHS services and systems. This group includes:
• social care services;
• voluntary sector providers;
• private sector care providers
• hospices;
• research organisations applying for section 251 approval;
• companies providing services to the NHS.

Information sharing partners may also include organisations that have no current requirement to carry out IG assessments or do not provide IG assurance in the same way, such as:

• the police;
• district & borough councils;
• the Department for Work and Pensions;

6. Information Sharing Agreements (ISA)

Information sharing agreements are sometimes known as information or data sharing protocols which set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. The Trust recognises that it is good practice to have Information Sharing Agreements in place, and to review them regularly, particularly where information is to be shared on a large scale, or on a regular basis.

All Information Sharing Agreements will describe:

• the purpose, or purposes, of the sharing;
• the legal basis for sharing
• the potential recipients or types of recipient and the circumstances in which they will have access;
• who the data controller(s) is and any data processor(s)
• the data to be shared;
• data quality including the accuracy, relevance and usability;
• data security;
• retention of shared data;
• individuals’ rights and the procedures for dealing with access requests, queries and complaints;
• any review of the effectiveness and termination of the sharing agreement;
• the sanctions for failure to comply with the agreement or breaches by individual staff.

7. Purposes for Sharing Information

The purposes for sharing personal information may include:

• Assuring and improving the quality of care, treatment and advice;
• Delivery of effective health care, treatment and advice;
- To safeguard children and vulnerable adults from harm;
- Monitoring and protecting public health, safety and well being;
- Risk management;
- Managing and integrating the planning of services
- Contracting and Commissioning the provision of services
- Auditing of accounts, care and performance;
- Investigating complaints or actual potential legal claims;
- Teaching and staff development;
- Statistical analysis;
- Research & Development.

8. **When is an ISA Required?**

Many organisations, in particular the NHS and Social Care are able to demonstrate they have an established IG framework in place by means of their IG Toolkit (IGT) assessed performance.

Partner organisations that are achieving an adequate level of performance (i.e. attainment level 2 or above against all requirements) can be regarded as ‘trusted’ organisations for information sharing purposes where the purpose of sharing is the delivery of care. These organisations will all be working to the same standards and will be taking appropriate action to satisfy legal requirements and hold information securely.

**Sharing for direct health-care purposes**

The Trust is not required to put in place Information Sharing Agreements where information sharing is between ‘trusted’ organisations for direct health-care purposes. Such agreements may still be of value where it may be important to establish working procedures or contact points to support day to day operational activity.

Where partner organisations are unable to demonstrate the required information governance performance to be classified as ‘trusted’, either because they are not mandated to complete the IG Toolkit or do not attain level 2 or above against all requirements, routine information sharing will require an Information Sharing Agreement. This is to ensure the rules are clearly understood and the requirements of law and guidance are being met.

**Sharing for non care purposes**

Information Sharing Agreements are required where information sharing is for non direct health-care purposes. Where the information sharing is between ‘trusted’ organisations, the agreement must include the secondary uses in question. This includes, for example, stating the purpose of information sharing, constraints on the re-use of information, the retention periods for holding the information and destruction policies.
Information proposed to be shared between ‘non trusted’ organisations will require an Information Sharing Agreement that addresses the required governance standards in the recipient organisation, the legal principles that apply. The agreement should also include the additional standards associated with the secondary uses in question, as detailed above relating to the purpose, constraints on re-use, retention periods and destruction of information.

The following table sets out when an ISA is required and when it is optional.

<table>
<thead>
<tr>
<th>Recipient organisation is achieving the required level of information governance performance</th>
<th>Sharing for direct health-care purposes</th>
<th>Sharing for non direct health-care purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>An ISA is optional</td>
<td>An ISA necessary that focuses on the secondary uses in question, i.e. the purpose, constraints on re-use of information, retention periods and destruction policies.</td>
<td></td>
</tr>
</tbody>
</table>

| Recipient organisation is unable to demonstrate the required information governance performance | An ISA is necessary that addresses the required information governance standards in the recipient organisation and the legal principles that apply. | An ISA is necessary that addresses the required governance standards in the recipient organisation, the legal principles that apply and the additional standards associated with the secondary uses in question, (i.e. the purposes, constraints on re-use of information, retention periods and destruction). |

9. **Factors to Consider before Sharing**

There are a number of factors the Trust will consider before entering into any information sharing in order to assess the objectives and any potential benefits or risks when deciding to share information or not:

- What is the sharing meant to achieve?
- What information *needs* to be shared?
- Who will have access to the personal information?
- How will the information be shared?
- What, if any, risks does sharing the information pose?
- Could the objective be achieved without sharing personal information?
- Will any of the information being shared be transferred outside of the European Economic Area?
10. Privacy Impact Assessments

Before entering into any data sharing agreement the Trust will consider carrying out a privacy impact assessment. This will help to assess the benefits the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

If an assessment is required the Trust will follow the Information Commissioners ‘Conducting Privacy Impact Assessments Code of Practice.

11. A Summary of Legal & NHS Mandated Frameworks for Sharing Information

Before any personal information is shared it is important to understand the legal framework in place to ensure the sharing is done ‘fairly’ and ‘lawfully’. There is no single source of law that regulates the powers that a public body has to use and to share personal information. The collection, use and disclosure of personal information are governed by a number of different areas of law as follows:

- The law that governs the actions of public bodies (administrative law);
- Data Protection Act 1998;
- Common Law Duty of Confidentiality;

12. The Data Protection Act 1998

The principal legislative provision relating to data protection is the Data Protection Act 1998 (DPA) which controls the use that can be made of personal data. The DPA gives individuals a number of important rights to ensure that personal information covered by the DPA are processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of data sharing.

The sharing of personal data is primarily governed by the Data Protection Act 1998. The DPA, imposes obligations upon “data controllers” (i.e. those who determine how personal data is held and used) when they are “processing” “personal data” and gives rights to “data subjects”. Sections 1 and 2 of the DPA define these concepts which are summarised below:

*Data* includes all electronically processed information as well as some manual records.

*Personal data* means data relating to an identified or identifiable living individual.
Sensitive personal data are personal data consisting of information as to
- racial or ethnic origin;
- political opinions, religious and similar beliefs,
- trade union membership;
- physical or mental health;
- sexual life;
- the commission or alleged commission by the data subject of any offence;
- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Many types of public sector data sharing will involve information held on computer, so if the information relates to identified or identifiable individuals, it will be clear that the DPA applies.

Data controllers” are person who determine the purposes for which and the manner in which, the personal data are processed.

Data processors” are persons who process personal data on behalf of a data controller, rather than on their own behalf.

Data subjects” are the individuals to whom the personal data relate.

Data sharing” refers to the processing of personal data by one data controller by giving it (or a copy of it) into the custody and control of another data controller or data processor.

12.1. Fair and Lawful Processing

Principle 1 of the Data Protection Act 1998 requires that 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.

Generally, personal data is not to be regarded as being processed ‘fairly’ unless the data subjects of the personal data is provided with (or has ready access to) certain pieces of information, either prior to, or at the time that the processing first takes place. The information must include:

- the identity of the Data Controller;
• the purpose or purposes for which the data is intended to be processed;
• any other information that is necessary to enable the particular processing to be fair.

Usually this requirement is complied with through the provision of a “Fair Processing Notices” which is drawn to the data subject’s attention when they supply their personal data to the data controller.

The Trust’s Fair Processing Notice is it’s information booklet ‘Your Information – Your Health Records’ which clearly informs patients about confidentiality and the way patient information may be used and shared. This booklet is available from patient areas within the Trust and from the Trust’s website:

The “lawfulness” requirement means that all relevant legal obligation, both statutory and under common law, must be complied with.

The processing of all personal data must be fair, lawful and meet one of the DPA’s Schedule 2 conditions, and a Schedule 3 condition for sensitive personal data.

12.2. Schedule 2 Conditions

At least one of the following 6 conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):

- The data subject has given their consent
- For the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The process is necessary to protect the vital interests of the data subject.
- For the exercise of any other functions of a public nature exercised in the public interest.
- To pursue legitimate interests of the controller unless prejudicial to interests of the data subject.

The following are Schedule 2 conditions of particular relevance to public sector data sharing.

Paragraph 1 - Consent of the data subject

“The data subject has given his consent to the processing”
Public bodies which share data may be able to rely on the consent of the data subject to satisfy Schedule 2 (and explicit consent in relation to Schedule 3 when processing sensitive personal data). While consent is the most conclusive of the conditions, it frequently cannot be met. Obviously where another Schedule 2 condition is applicable, it is not necessary to obtain consent. In certain circumstances (such as data sharing in the context of regulatory or enforcement functions) it is unlikely that consent would be an appropriate condition and public bodies are likely to rely on other conditions.

**Paragraph 3 - Compliance with a legal obligation**

*The processing is necessary…. to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*

This provision covers legal obligations arising from another source other than contract, including statute, EU law or the common law. “Necessary” in this context does not mean “absolutely essential”. If there is a relevant statutory gateway that imports a legal obligation to disclose data, then this condition is likely to apply. For example, it would be relevant to data processing by public bodies that are under a legal obligation to provide relevant information to the National Audit Officer under section 8 of the National Audit Act 1983.

**Paragraph 5(a) - administration of justice**

*“The processing is necessary….for the administration of justice”*

This condition is likely to apply to a wide range of processing activities carried out by courts, tribunals and other bodies that have judicial functions. It would, for example, permit a court to provide a defendant’s criminal and other records to a lawyer appointed by the court at short notice to represent a defendant at a hearing following the execution of an arrest warrant.

**Paragraph 5(b) - functions conferred by or under an enactment**

*“The processing is necessary….for the exercise of any functions conferred on any person by or under any enactment”*

This condition will include processing carried out pursuant to express statutory powers or reasonably required or ancillary to the exercise of express or implied statutory functions.

When data are shared there are two instances of processing, one by the body making the disclosure and the other by the recipient. Each of these bodies must comply with the DPA, and in particular both bodies must have the appropriate “vires” (power). The first to disclose and the second to receive and further process the data. For the purposes of paragraph 5(b) what matters is the overall objective of the sharing, rather than the specific objective of either body.
As explained above, “necessary” in this context does not mean “absolutely essential”, and data sharing may meet this condition if it is a reasonable and proportionate way for a public body to give effect to its functions.

**Paragraph 5(c) - functions of central government**

“*The processing is necessary... for the exercise of any other functions of a public nature exercised in the public interest by any person*”

This condition will cover processing relating to functions carried out by central government departments and offices that derive from the Crown’s common law or statutory powers. It is probably the most common used condition for all data processing by central government departments and offices that derive from the Crown’s common law or statutory powers.

**Paragraph 5(d) - Other public functions**

“*The processing is necessary... for the exercise of any other functions of a public nature exercised in the public interest by any person*”

Similar considerations apply to this condition as to paragraphs 5(b) and (c), but the condition is more broadly applied. This condition would, for example, cover processing by voluntary organisations or private bodies provided it is in support of a public function that is in the public interest.

**Paragraph 6 (1) - Legitimate interests of the data controller**

“*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, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.*”

The concept of “legitimate interests” is not defined in the DPA and could potentially have very wide applications. It involves a case by case consideration of the balance between the legitimate interests of the data controller and the data subject. In most cases where data sharing by a public authority could satisfy this condition, it is likely to satisfy one of the other, more specific, conditions explained above. Public bodies should only rely on this condition where no other condition can be satisfied. The NHS may have a number of legitimate interests that could be relevant, including preventing and investigating fraud or the misuse of its services and the processing of administrative data for research purposes.

### 12.3. Schedule 3 Conditions

At least one of the following 20 conditions must be met in the case of all processing of sensitive personal data (except where a relevant exemption applies): -
The following are Schedule 3 conditions of particular relevance to public sector data sharing

If sensitive personal data are being shared, one of the conditions of Schedule 3 must also be fulfilled. Some of the conditions in Schedule 3 closely mirror those in Schedule 2, and there is no prohibition on relying on similar conditions in both Schedules, providing of course that they are properly fulfilled; there are slight differences in wording that must be considered.

**Paragraph 1: Explicit consent**

“The data subject has given explicit consent to the processing of personal data”

Consent may form the basis for legitimate data sharing. In relation to Schedule 3, the consent must be “explicit”. 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.

Public bodies should satisfy themselves when relying on this condition that the individual was fully aware of all the relevant details of the proposed sharing. This should, at a minimum include details of exactly what will be shared, with whom, on what basis and for what purpose.
Paragraph 7(1): Public functions

“The processing is necessary for (a) the administration of justice, (b) for the exercise of any functions conferred on any person by or under any enactment, or (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department”

The conditions set out in paragraph 7(1)(a), (b) and (c) of Schedule 3 are worded in a similar way to those set out in paragraph 5(a), (b) and (c) of Schedule 2 respectively, considered above.

Paragraph 8: Medical Purposes

The processing is necessary for medical purposes and is undertaken by:

(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

“Medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

Where processing is solely for social care or other Local Authority purposes it is unlikely that Schedule 3(8) would apply as the definition relates to medical purposes. However in the context of the integrated care agenda, it is increasingly likely that this will include a combination of both social care and medical purposes. Therefore, processing in such contexts will be permitted under Schedule 3(8) so long as the social care being provided has a health element, focus or outcome (whether that be public or individual).¹

Paragraph 9: Research data

The processing –

(a) Is in the substantial public interest:
(b) Is necessary for research purposes (which expression shall have the same meaning as in section 33 of the DPA);
(c) Does not support measures or decision with respect to any particular data subject otherwise than with explicit consent of the data subject: and
(d) Does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person

Specially with regard to the processing of sensitive personal data for research purposes, one of the Schedule 3 conditions for lawful processing of such data

¹ http://systems.hscic.gov.uk/infogov/iga/resources/nhsnumber2.pdf
relates to research activities that are ‘in the substantial public interest’. This condition is contained in the Data Protection (Processing of Sensitive Personal Data) Order 2000, SI 200/417 made under the DPA.

In order to help understand what is in the ‘substantial public interest’ it is useful to firstly give consideration to what is in the ‘public interest’ (Refer to Section 14.2.)


The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable action within their powers (which would include information sharing) to safeguard the Convention rights of children. These rights include the right to life (Article 2), the right not to be subjected to torture or inhuman or degrading treatment (Article 3) and the right to liberty and security (Article 5).

Article 8 of the European Convention on Human Rights was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect for private and family life:

- **Article 8.1:** Everyone has the right to respect for his private and family life, his home and his correspondence.

- **Article 8.2:** There shall be no interference by a public authority with exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, protection of health and morals or for the protection of rights and freedoms of others.

Sharing confidential information may be a breach of an individual’s Article 8 right: the question is whether sharing information would be justified under Article 8.2 and proportionate.

The right to a private life can be legitimately interfered with where it is in accordance with the law and, for example, is necessary for the prevention of crime or disorder, for public safety or for the protection of health or morals, or for the protection of the rights and freedoms of others. You need to consider the pressing social need and whether sharing the information is a proportionate response to this need and whether these considerations can override the individual’s right to privacy. If a child or young person is at risk of significant harm, or sharing is necessary to prevent crime or disorder, breach of the child or young person’s right could be justified under Article 8.
14. Common Law Duty of Confidence

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as ‘judge-made’ or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent.

In practice this means that all patient information, whether held on paper or electronically, must not normally be disclosed without consent.

The following four circumstances making disclosure of confidential information lawful are:

1. Where the individual has given their consent.
2. Where disclosure is necessary to safeguard the individual, or others, or is in the public interest;
3. Where there is a legal duty to do so, for example a court order; and
4. Where there is a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006.

The Confidentiality: NHS Code of Practice describes the circumstances in detail, however these have been summarised in the following sections below.

14.1. Consent

Where no legal basis to share information can be found, consent must be gained from the individual who must fully understand the decisions they are making. They will need to be made fully aware of:

- The nature of the information that will be shared
- Who the information will be shared with
- The purposes for which the information will be used
- Other relevant details including their right to withhold or withdraw consent
- The potential consequences of not sharing information

Types of consent

**Implied consent** is a controversial form of consent which is not expressly granted by a person, but rather inferred from a person's actions and the facts and circumstances of a particular situation (or in some cases, by a person's silence or inaction). An example is an appointment made with a GP by a patient with a physical complaint; it is implied that by making the appointment
the patient gives consent to the physician to make a diagnosis and offer treatment.

**Express consent** is clearly and unmistakably stated, rather than implied. It may be given in writing, by speech (orally), or non-verbally, e.g. by an unambiguous gesture such as a nodding in context. Non-written express consent not evidenced by witnesses or an audio or video recording may be disputed if a party denies that it was given.

- Informed Consent in medicine is consent given by a person who has a clear appreciation and understanding of the facts, implications, and future consequences of an action.

For consent to be valid, it must be voluntary and informed, and the person consenting must have the capacity to make the decision. These terms are explained below:

- **Voluntary** – the decision to either consent or not to consent to treatment must be made by the person themselves, and must not be influenced by pressure from medical staff, friends or family.

- **Informed** – the person must be given all of the information in terms of what the treatment involves, including the benefits and risks, whether there are reasonable alternative treatments and what will happen if treatment does not go ahead.

- **Capacity** – the person must be capable of giving consent, which means they understand the information given to them, and they can use it to make an informed decision.


### 14.2. Public Interest

Under a common law duty of confidentiality, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

It is advised that records are kept of any such disclosures so that there is clear evidence of the reasoning used and the circumstances prevailing. Disclosures in the public interest should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the organisations they work within.
Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against his/her wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

Decisions will sometimes be finely balanced and staff may find it difficult to make a judgement. The Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest. If in doubt staff should seek guidance from the Caldicott Guardian or the Information Governance department.

The following are some examples of disclosures made in the public interest.

Serious Crime and National Security

The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Risk of Harm

Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face.

Examples of where public interest can be a defence include:

- Reporting to the Driver & Vehicle Licensing Centre a patient who rejects medical advice not to drive (although health professionals should inform the patient of their intention to report it);
- Breaching the confidentiality of a patient who refuses to inform his or her sexual partner of a serious sexually transmissible infection;
- Releasing relevant confidential information to social services where there is a risk of significant harm to a child.

2 Serious crime, as defined by the GMC is “a crime that puts someone at risk of death or serious harm and would usually be crimes against the person, such as abuse of children” (GMC guidance “Confidentiality: Protecting and Providing Information paragraph 37).

In order for any processing of sensitive personal data for research purposes to be considered as in the **substantial public interest** and satisfy the condition set out in paragraph 9 of the Data Protection(Processing of Sensitive Personal Data) 2000 Order, it is likely to have to be able to demonstrate that:

- It serves the interest of society as a whole
- It promotes openness and transparency by public bodies, whilst also protecting individuals' personal data.
- The public attaches some importance to the information being processed
- Individuals are not caused any substantial damage or distress, albeit that damage and distress to a data subject is not always tangible and quantifiable.

An example of where substantial public interest can be a defence is the transmission of relevant patient files by hospitals to local authority cancer registries, because it is vital in protecting and enhancing public health.

### 14.3. Statutory Gateways

Most public sector organisations, other than government departments headed by a minister of the Crown (which have common law powers to share information), derive their powers entirely from statute – either from the Act of Parliament which set them up or from other legislation regulating their activities.

Relevant legislation will define the functions of a public authority in terms of its purposes, the things that it must do, and the powers which the organisation may exercise in order to achieve those purposes. Therefore it is necessary to identify where the data sharing in question would fit, if at all, into the range of things that the organisation can do.

Some Acts of Parliament give public bodies **express statutory obligations and powers** to share information. These are often referred to as ‘gateways’ and are enacted to provide for the sharing of information for particular purposes. These gateways may be permissive or mandatory.

- An example of a ‘permissive statutory gateway’ is Section 115 of the Crime and Disorder Act 1998, this **permits** people to share information to help prevent or detect crime.

- An example of a ‘mandatory statutory gateway’ is Section 8 of the National Audit Act 1983, which **imposes a legal obligation** on public bodies to provide relevant information to the National Audit Office.

Where there is no express statutory power to share information it may still be possible to **imply** such a power from the other duties and powers public bodies have. Many activities of statutory bodies will be carried out as a result of **implied statutory powers**, particularly as it may be difficult to expressly
define all the numerous activities that a public body may carry out to deliver its main duties and powers.

Having express or implied statutory powers in any particular case does not mean that the Human Rights Act 1998, the common law duty of confidentiality, and the Data Protection Act 1998 can be disregarded. Having a mandatory statutory gateway does however mean that confidential information can be shared without either consent or the public interest test needing to be applied, but this will be rare and generally in limited circumstances.

The relevant legislation usually defines the organisation’s functions in terms of its purposes and the powers which the organisation may exercise in order to achieve those purposes.

15. Legislation that Impacts on the NHS

The following are some examples of legislation in place that contain express powers or which imply powers to share information impact on NHS organisations.

- Children Act 1989
- Children Act 2004
- Criminal Justice Act 2003
- Crime and Disorder Act 1998
- Health & Social Care Act 2012
- Health & Social Care (Safety & Quality) Act 2015
- Mental Capacity Act 2005
- National Health Service Act 1977
- National Health Service Act 2006
- NHS Act 2006

16. Monitoring & Audit

The IG Toolkit contains guidance on expected standards and key performance indicators, which together will be used to monitor the effectiveness of this policy.

The Information Governance Manager is responsible for monitoring compliance with this policy and ensuring its effectiveness.

The content of this policy will be audited annually against the IG Toolkit and by Internal and External Audit.
17. References

Department of Health: Information: To share or not to share? The Information Governance Review: 

Department of Health: NHS Information Governance Guidance on Legal Professional Obligation 
http://systems.hscic.gov.uk/infogov/codes/lglobligat.pdf

Department of Health: The Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures 

Information Commissioner: Conducting Privacy Impact Assessments – Code of Practice 

IG Toolkit https://www.igt.hscic.gov.uk/
### Equality Impact Assessment

<table>
<thead>
<tr>
<th></th>
<th>Yes/No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the policy/guidance affect one group less or more favourably than another on the basis of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Ethnic origins (including gypsies and travellers)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Nationality</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Religion or belief</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Sexual orientation including lesbian, gay and bisexual people</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Disability - learning disabilities, physical disability, sensory impairment and mental health problems</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Marriage &amp; Civil partnership</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Pregnancy &amp; maternity</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is there any evidence that some groups are affected differently?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is the impact of the policy/guidance likely to be negative?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>If so can the impact be avoided?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>What alternatives are there to achieving the policy/guidance without the impact?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Can we reduce the impact by taking different action?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If you have identified a potential discriminatory impact of this procedural document, please refer it to (Insert name and position) together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact (Insert name and position).
Policy and Procedure Sign-off Sheet

<table>
<thead>
<tr>
<th>Signature</th>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Policy Name and Number: Information Sharing Policy

Version Number and Date: January 2016

No: 1

Service Location:

All staff members must sign to confirm they have read and understood this policy.