Information Sharing Policy

NHS England and NHS Improvement

Information Sharing Policy

Version number: v4.1

First published: March 2019

Updated: September 2019

Prepared by: Corporate Information Governance

Classification: OFFICIAL

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact england.ig-corporate@nhs.net

NHS England and NHS Improvement INFORMATION READER BOX

Directorate		
Medical	Operations and Information	Specialised Commissioning
Nursing	**Trans. & Corp. Dev.**	Strategy & Innovation
Finance		

Publications Gateway Reference:	
Document Purpose	Policy
Document Name	Information Sharing Policy
Author	Corporate Information Governance
Publication Date	September 2019
Target Audience	All NHS England and NHS Improvement Employees
Description	Policy and high-level procedures for Information Sharing
Superseded Docs (if applicable)	Information Sharing Policy V4.0
Action Required	To note
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	Carol Mitchell Head of Corporate Information Governance Quarry House Leeds LS2 7UE England.ig-corporate@nhs.net

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Contents

1 Introduction

Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services. The Caldicott Review 'To share or not to share' specified that "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 the Caldicott principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Government has also emphasised the importance of data. The Review of Data Security, Consent and Opt-Outs published by the National Data Guardian in 2016 introduced ten Data Security Standards. These form the basis for the Data Security and Protection Toolkit.

The EU General Data Protection Regulation (GDPR), and Data Protection Act 2018 (DPA 2018) which implements it in the UK, has strengthened the legislation, in particular requiring that organisations are accountable and able to demonstrate compliance. Please refer to the Information Commissioner's web site and IGA GDPR guidance. References to data protection legislation in this policy include provisions of the GDPR and DPA2018.

It is important that NHS England and NHS Improvement protects and safeguards person-identifiable information that it gathers, creates processes and discloses, to comply with the law, relevant NHS mandatory requirements and provide assurance to patients and the public.

An explanation of what is meant by information sharing can be found in Section 4. All employees working in the NHS are bound by the common law duty of confidence and must comply with data protection legislation. Staff must handle personal information they may come into contact with during the course of their work in a lawful and compliant manner. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation. It is important for staff to be aware that it is an offence under DPA2018 for a person knowingly or recklessly to obtain or disclose personal data – see Annex A.

This policy sets out the requirements placed on all NHS England and NHS Improvement staff when sharing personal information within the NHS and between the NHS and other bodies.

The Information Commissioner's Office (ICO) has issued a data sharing code of practice that must be adhered to when sharing personal data.

Information can relate to patients, staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number etc. This type of information must not be stored on removable or mobile media unless it is encrypted as per current NHS encryption guidance or a business case has been approved by the Corporate Information Governance Team (england.ig-corporate@nhs.net).

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records etc.

NHS England and NHS Improvement are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how we will deliver integrated care to patients at the local level, how we set the whole of the NHS up to do that and how it will benefit patients and communities. To make this work we need to perform some functions of the individual organisations together, achieving seamless integration of our working practices. Where the functions require processing of personal data, the cooperating organisations may be individually or jointly responsible for the processing – as *controllers* or *joint controllers* as defined by the GDPR. Section 6 summarises the requirements of our Joint Controller and Information Sharing Framework Agreement.

The Legal and NHS Mandated Framework for information sharing which forms the key guiding principles of this policy can be found in Appendix A.

2 Scope

All our staff and of hosted organisations, without exception, are within the scope of this policy, including and without limitation:

- Central and Regional Teams;
- All Commissioning Support Units;
- NHS Interim and Management Support (NHS IMAS);
- NHS Sustainable Development Unit;
- Strategic Clinical Networks;
- Clinical Senates; and
- Healthcare Safety Investigation Branch (HSIB).

The personal information within scope of this policy includes:

- Personal Data – as defined by the GDPR as identifiable information about living individuals (including pseudonymised personal data)
- Personal Confidential Data (PCD) – taken from the Caldicott Review.

PCD describes information about identified or identifiable individuals, which should be kept private or secret. It includes data within the scope of the GDPR definition of

personal data and also identifiable information about the deceased which may be subject to the common law duty of confidence (confidentiality).

3 Aims of the policy

The aims of this policy are to:

- Provide a framework for NHS England and NHS Improvement, and those working on its behalf to:
    - provide information to deliver better care
    - consider the controls needed for information sharing
    - ensure the expected standards are met (including that partners to information sharing are aware of the obligations of consent or how to take appropriate account of an individual's objection)

- Set out NHS England's and NHS Improvement's agreed framework for processing personal data in support of their joint working enterprise, with reference to commitments we have made in our Joint Controller and Information Sharing Framework Agreement.

4 Information Sharing

Information sharing, in the context of this policy, means

1. routine disclosure or receipt of personal information by NHS England or NHS Improvement, individually or jointly to or from another organisation or organisations. This can take the form of:

    - a reciprocal exchange of information;
    - one or more organisations providing information 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.

2. routine processing of personal data by NHS England or NHS Improvement, jointly or as individual controllers, in support of their joint working enterprise (see section 6).

3. exceptional, one-off disclosures of data in unexpected or emergency situations.

Sharing of non-personal information
Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared.

Anonymous or aggregate (numbers) information may be shared internally or with other organisations for example to: improve patient experience; facilitate commissioning of services; manage and plan future services; facilitate quality improvement and clinical leadership; assure and improve the quality of care and treatment; statutory returns and requests; train staff; audit performance.

Regard must be had to the document "Anonymisation standard for publishing health and social care data specification" which specifies the steps required to select an appropriate anonymisation plan and to assess re-identification risk (refer to the ICO anonymisation code of practice for further information).

Sharing personal information with other organisations
Necessary and proportionate, personal information may be shared with other organisations for example to: investigate complaints or potential legal claims; protect children and adults at risk; assess need, service delivery and treatment.

This policy covers two main types of information sharing:

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

Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to exceptional, one-off decisions about sharing.

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

Exceptional or 'one-off' information sharing. Much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. All ad-hoc or one-off sharing decisions must be carefully considered and documented. Please see Section 7 for further details.

Factors to consider. When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you should consider **what is**

the sharing meant to achieve? There should be a clear objective or set of objectives. Being clear about this will identify the following:

- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.
- **What information needs to be shared?** You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "**Use the minimum necessary personal confidential data**".
- **Who requires access to the shared personal data?** You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.
- **When should it be shared?** Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
- **How should it be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- **How can we check the sharing is achieving its objectives?** You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
- **How are individuals made aware of the information sharing?** Have individuals been provided with the fair processing information as required by the GDPR? How is it ensured that individual's rights are respected and can be exercised e.g. how can they access the information held once shared?
- **What risk to the individual and/or the organisation does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
- **Is the information subject to the National Data Opt-out Programme?** If a patient has exercised their rights under this programme, care must be taken not to share that data. Further information can be found on the NHS Digital website.
- **What is the legal basis for data protection purposes?** Organisations must identify the lawful basis (e.g. meeting statutory duties) for processing and, where necessary, a condition for processing special categories data (e.g. managing a health and care service).
- **If the information is confidential**, what is the legal basis that complies with the common law duty of confidence? This can be consent (implied or explicit), overriding public interest or required or permitted by law.

It is good practice to document all decisions and reasoning related to the information sharing.

For any assistance and guidance, and if in any doubt about when it is appropriate to share information please contact the Corporate Information Governance team. CSU staff should consult local IG resources.

In all circumstances of information sharing, staff will ensure that:

- When information needs to be shared, sharing complies with the law, guidance, best practice is followed and an information sharing agreement is in place;
- Only the minimum information necessary for the purpose will be shared;
- Individuals' rights will be respected, particularly confidentiality, security and the rights established by the GDPR;
- Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure;
- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

5 Information Sharing Agreements

Information sharing agreements, sometimes known as 'Information sharing protocols' or 'data sharing protocols', set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have an information sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An information sharing agreement must, at least, document the following:

- the purpose, or purposes, of the sharing;
- the legal basis for sharing under the DPA2018/GDPR;
- the legal basis to comply with the common law duty of confidence;
- 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) (see Appendix A)
- the data to be shared;
- data quality – accuracy, relevance, usability;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, other applicable GDPR rights, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected sanctions for failure to comply with the agreement or breaches by individual staff.

An information sharing agreement should be used when NHS England or NHS Improvement, acting as data controller, is sharing information directly with other organisations that will act either as a joint data controller with NHS England/NHS Improvement, or as data controllers in their own right for that information.

Any processing by an organisation on behalf of NHS England or NHS Improvement shall be governed by a data processing agreement, **not** an information sharing agreement. The GDPR requires a contract, or other legal act that is binding on the processor with regard to NHS England or NHS Improvement as data controller, that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Sharing for Non-care Purposes – There are requirements where confidential personal information needs to be shared for non-care purposes. Whether sharing with a "trusted organisation[1]" or not, the purposes for sharing need to be specifically documented and limited, and additional requirements such as recorded consent or evidence of support under Section 251 of the NHS Act 2006 may be required to enable lawful sharing.

In particular, when sharing information for 'non-care purposes' – often referred to as secondary uses (e.g. for purposes including commissioning, healthcare development, improving NHS resource efficiency etc.), the NHS Digital guidance 'A guide to confidentiality in health and social care' and the NHS Digital 'Secondary Use Services Guidance' (both referenced in section 11.2) both need to be complied with before any potential information is shared.

The **Caldicott Report** and subsequent **2013 Review** recommends information sharing agreements should be developed between organisations sharing personal identifiable information.

Where it is decided that an Information Sharing Agreement needs to be documented between organisations there is a template agreement available from the Corporate Information Governance department intranet pages for NHS England and NHS Improvement staff. This agreement covers the sharing of personal identifiable information and explains the process for signing off the agreement.

The next section includes a summary of the Joint Controller and Information Sharing Framework Agreement between NHS England and NHS Improvement.

6 Joint working

NHS England and NHS Improvement are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how we will deliver integrated

[1] Further information can be found in" DSP IR Guidance"

care to patients at the local level, how we set the whole of the NHS up to do that and how it will benefit patients and communities.

To make this work we need to perform some functions of the individual organisations together, achieving seamless integration of our working practices. Where the functions require processing of personal data, the cooperating organisations may be individually or jointly responsible for the processing – as *controllers* or *joint controllers* as defined by the GDPR. An organisation is a controller where it determines the purpose and means of the processing.

To ensure that we comply with our data protection obligations the three statutory organisations (NHS England and NHS Improvement – which comprises Monitor and TDA) have entered into a Joint Controller and Information Sharing Framework Agreement. This sets out our joint data protection responsibilities and the measures that we have put in place to ensure that we comply, including:

- Appointment of joint Data Protection Officer and support function
- Appointment of a joint Senior Information Risk Owner
- Requirement to collaborate in conducting data protection impact assessments before introducing new joint working practices
- A shared information asset register
- Requirement to collaborate in provision of appropriate privacy information to data subjects.

The agreement includes scenarios in which we act either as individual or joint controllers when processing personal data in support of joint working – depending on whether purposes are determined jointly or by one controller and including the possibility of a 'processor' relationship – where one organisation acts on instructions of another.

These scenarios provide a focus for those completing DPIAs for their proposed collaborative working initiatives and are listed below.

1. Joint controllers – aligned exercise of separate and specific statutory functions
2. Joint controllers – general powers and corporate governance arrangements
3. One organisation is a controller, supported by staff employed by any of the other organisations
4. Data sharing – with each organisation acting as a separate sole Controller
5. Processor – one or more of the organisations acts as a processor for one or more of the others.

What this means for an individual staff member is that he or she may act for any of the three statutory organisations (controllers) individually, or jointly as follows:

- Scenarios 1 and 2 – for multiple controllers working on the jointly exercised functions
- Scenario 3 – only for the controller whose function is being performed

- Scenario 4 – for either the disclosing or the recipient controller (but not both)
- Scenario 5 – for the recipient processor acting entirely on the instructions of the disclosing controller.

In each of these scenarios, for individual staff it makes no difference who their employing organisation is. What is important is that it is clear who the controller organisation(s) is/are, and the purposes for which personal data are being processed under its authority.

The day to day work of our joint teams should not be affected by any mix of organisations employing individual staff – in scenarios 1, 2 and 3 the operation of our joint teams should be seamless. To enable this, managers are responsible for making sure that their staff in their teams have a clear understanding of the purposes for which they are processing personal data, and that they must not disclose or otherwise process personal data for any other purpose – irrespective of their employing organisation.

In scenario 4 where personal data is shared between organisations for their separate individual purposes, it is the responsibility of the manager or business lead for the function to ensure that an information sharing agreement is in place (see section 5).

In scenario 5, where an organisation is to act as a processor for one or more o fthe other organisations, it is the responsibility of the manager or business lead for the function to ensure that a data processing agreement is in place using the standard template.

Data protection impact assessment is a key tool in ensuring that the purposes, legal basis, and organisational responsibilities for processing are clearly documented. A DPIA must be conducted before any new processing is introduced (see section 7). Conducting DPIAs is also essential to ensure that we have a corporate record of the processing activity and have provided appropriate privacy information.

We will publish guidance on conducting DPIAs which addresses the 5 scenarios listed above.

7 Data Protection Impact Assessment

Before establishing a new process that involves processing of personal data including information sharing, a data protection impact assessment (DPIA) must be conducted. This is a legal requirement under the GDPR where there may be a high risk to individuals. NHS England's and NHS Improvement's DPIA template includes screening questions to assess whether there is a high risk and so whether a full DPIA is required.

A DPIA helps to assess the benefits that the information sharing might bring to particular individuals or society more widely, and balance against any risks to individuals arising from processing their data. It also ensures that the appropriate legal bases are identified and documented. It identifies risks or potential negative

effects, such as non-compliance with data protection legislation, an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on DPIAs can be found within the Information Governance requirements for New Processes, Services, Information Systems and Assets.

Any new information assets and data flows that arise out of a new project or procurement where NHS England or NHS Improvement is the data controller or receives personal, confidential, sensitive or business sensitive information will need to be recorded as part of NHS England's and NHS Improvement's Information Asset Register, within the Information Asset Management System (IAMs). Further information around this can be found at the following intranet location.

8 Further advice

With information sharing there will always be exceptional and difficult circumstances where advice may be needed. The Data Protection Officer, local Caldicott Guardian or Corporate Information Governance specialist should be consulted where there are any concerns about whether the proposed information sharing is appropriate. These staff will use their judgement and knowledge of the law and practice to act in the best interests of patients/clients. The issue, subsequent decisions and actions should be documented within NHS England's and NHS Improvement's Caldicott Log. Please contact your local Information Governance team member around any exceptional needs or requests for information sharing, and any information sharing decisions that may require the Caldicott Guardian's input.

9 Distribution and Implementation

9.1 Distribution Plan

This document will be made available to all staff via the intranet site. A notice will be issued in the staff bulletin notifying of the release of this document.

9.2 Training Plan

The Corporate Information Governance team's training needs analysis plan will cover necessary elements of information sharing.

10 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Corporate Information Governance team, together with independent reviews by both Internal and External Audit on a periodic basis.

The Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document.

11 Equality Impact Assessment

This document forms part of NHS England's and NHS Improvement's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified.

12 Associated Documents

The following documents will provide additional information:

- Acceptable Use of ICT and User Obligations
- Confidentiality Policy
- Corporate Document and Records Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Security Policy

12.1 External reference documents

REF NO	ORGANISATION	TITLE	VERSION/ DATE
1	Information Commissioner's Office	Data Sharing: Code of Practice	May 2011
2	Information Commissioner's Office	https://ico.org.uk/media/1061/anonymisation-code.pdf	
3	Information Commissioner's Office	Data protection impact assessments	
4	NHS Digital	A guide to confidentiality in health and social care: references	V1.1 – September 2013
5	NHS Digital	Secondary use service	Multiple guidance documents on web
6	Ministry of Justice	Public Sector Data Sharing: Guidance on the Law	November 2003
7	Department of Health	NHS Information Governance: Guidance on Legal and Professional Obligations	September 2007
8	Information Standards Board	Anonymisation Standard for Publishing Health and Social Care Data Specification (Process Standard)	25/02/13
9	Information Governance Alliance	Information Governance Alliance	
10	General Medical Council	Confidentiality	

Appendix A: Summary of Legal and NHS Mandated Frameworks

NHS England and NHS Improvement is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of NHS England and NHS Improvement, who may be held personally accountable for any breaches of information security for which they may be held responsible. NHS England and NHS Improvement shall comply with the following legislation and guidance as appropriate:

Public Sector Data Sharing: Guidance on the Law

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. Some relevant legislation includes:

- the law that governs the actions of public bodies (administrative law);
- the Data Protection Act 2018;
- the EU General Data Protection Regulation – brought in to UK law by the DPA2018;
- the Human Rights Act 1998 and the European Convention on Human Rights;
- the common law duty of confidence.

The interrelationship between the above areas of law is quite complex. The starting point is always to determine whether the public body has the power to carry out any proposed data sharing. This will be a matter of administrative law.

The relevant legislation will probably define the organisation's functions 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, the things that it may do. So it is necessary to identify where the data sharing in question would fit, if at all, into the range of things that the organisation is able to do. Broadly speaking, there are three ways in which it may do so:

- **Express obligations** – Occasionally, a public body will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances but, where such an obligation applies, it is clearly permissible to share the information.
- **Express powers** – Sometimes, a public body will have an express power to share information. Again, an express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".
- **Implied powers** – Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express

provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental", and then check that the organisation has the power to engage in that activity.

The legal framework that applies to **private and third sector organisations** differs from that which applies to public sector organisations, which may only act within their statutory powers. However, all bodies must comply fully with the data protection principles. (See the Data Protection Act below).

Whatever the source of an organisation's power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question – otherwise, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. This might be the case where an NHS trust sets aside a duty of confidence because a doctor believes that a patient has been involved in serious crime. Whilst a disclosure in the public interest may be defensible in a particular case, this does not constitute a legal power to share data. It is best to proceed with caution when using public interest as a justification for sharing personal or sensitive data. Please contact the local Information Governance Team for further advice and guidance.

It is also important to ascertain 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.

The next stage is then to consider whether the proposed data sharing might nevertheless be unlawful due under the Data Protection Act 2018, Human Rights Act 1998, or the common law tort of breach of confidence.

The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018

The GDPR and DPA 2018 apply to living individuals and gives those individuals several important rights to ensure that personal data is 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 information sharing. Key principles in the GDPR and DPA 2018 that are relevant to information sharing are, personal information must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and where necessary kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, and;
- processed in a manner that ensures appropriate security of the personal data.

The GDPR also introduces the principle of accountability: The controller shall be responsible for and be able to demonstrate compliance with the principles.

The legislation gives rights to 'data subjects' including transparency (e.g. to be provided with privacy notices) and access to information held about them. There are other rights such as the right to object, which apply depending on the legal basis that applies.

Chapters 1 and 2 of the GDPR define these concepts:

The personal information within scope of this policy includes:

- Person identifiable data/information e.g. staff records
- Personal confidential data (PCD) - taken from the Caldicott Review

PCD describes information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the DPA 2018 definition of personal data but, for the purposes of this policy, it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'special categories' of personal data as defined in the DPA 2018.

'Personal data' 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Pseudonymised data' - The GDPR states clearly that pseudonymised data is 'personal data' and as a consequence the GDPR fully applies to pseudonymised data. However, the GDPR also states (in Recital 26) that data which is anonymised in such a way that individuals cannot be identified does not fall within the scope of the Regulation.

From this the important issue to be considered is around the fluid state of pseudonymisation. For example, if NHS Digital pseudonymises data and then goes onto make further use of that pseudonymised data, then in the eyes of the law the data will always be 'personal data'; albeit once pseudonymised the law recognises

this action as an increased form of protection/security. Ultimately though NHS Digital will have the key to the data and hence be capable of re-identifying the data.

However, if the same data set were to be disseminated to a third-party, then the data, on receipt, might not be classed as 'personal data'. For this to be the case the data must be subject to controls (technical and legal) to ensure there is no reasonable likelihood of re-identification. If those conditions can be met then the current ICO view is that this data is de-personalised in such a way that it falls out of the scope of the GDPR (and Data Protection Act 2018).

'Special categories of 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, and the commission or alleged commission of any offence or criminal proceeding. The GDPR imposes additional requirements in relation to the processing (including the sharing) of such data.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

'Controllers' are persons who determine the purposes for which, and the manner in which, the personal data are processed.

'Processors' are persons who process personal data on the instructions of a controller for the controller's purposes. They may not process the data for which they are instructed by the controller for their own purposes.

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

Click here for an online link to the Data Protection Act 2018

Offence of unlawful obtaining or disclosure etc.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller
(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained

Human Rights Act 1998

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature. Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal data. Article 8 is not an absolute right – public authorities are permitted to interfere with it if it is lawful and proportionate to do so.

It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing engages Article 8 or any other Convention right. However, if you disclose or share personal data only in ways that comply with the DPA2018 and common law duty of confidence, the sharing or disclosure of that information is also likely to comply with the HRA.

Click here for an online link to the Human Rights Act 1998

The 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 that 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/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client. It is irrelevant for example how old the patient/client is, or what the state of his/her mental health is; the duty still applies.

The Mental Capacity Act Code of Practice gives guidance for decisions made under the Mental Capacity Act 2005. Staff should comply with this when information is to be shared about individuals who may lack capacity.

The principle of Gillick competence applies when considering a child's ability to consent to treatment, and applies similarly to information sharing.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;

- where disclosure is necessary for an overriding public interest such as to safeguard the individual, or others; or

- where there is a legal duty to do so, for example a court order, or a permissive power such as s251 support.

Implied consent may be assumed where sharing of information for the purposes of providing direct care. However, this is only valid where appropriate information has been provided to the patient about the proposed sharing, or the activity is obvious – to ensure that the consent is informed.

Therefore, under the common law, a health or social care provider wishing to disclose a patient's/client's personal information to anyone outside the team providing care, or for non-care purposes should first seek the consent of that patient/client.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding safeguarding interest of the individual or others or in the public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.
Disclosures required by court order should be referred to the organisation's legal advisors as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested.

If a disclosure is made which is not permitted under common law the patient/client could possibly bring a legal action not only against the organisation but also against the individual responsible for the breach.

Section 251

Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes.

The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' actually refer to approval given under the authority of the Regulations.

Section 251 was established to enable the common law duty of confidentiality to be set aside to enable disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent was not practical, having regard to the cost and technology available.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant in relation to this policy is:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask, and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Click here for an online link to NHS Care Record Guarantee

Where there is any doubt, the Corporate Information Governance department can advise on whether a legal basis to share information exists.

Version control tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	July 2014	Information Governance Taskforce	Draft	New policy
2.0	June 2016	Head of Corporate Information Governance	Approved	Yearly review
3.0	July 2018	Data Protection Officer	Draft	Post-GDPR Review
4.0	March 2019	Information Governance Manager (NHSI)	Draft	Reviewed for NHS Improvement alignment
4.1	September 2019	IG Manager and Senior Corporate IG Lead	Approved	Amendments to reflect joint working and advice from Counsel