NHS England

Information Sharing Policy

Information Sharing Policy – personal information

Issue Date: June 2016

Document Number: POL_1016

Prepared by: Jenny Spiers – Information Governance Taskforce

Information Reader Box

Directorate	Purpose
Medical	Tools
Nursing	**Guidance**
Patients & Information	Resources
Finance	Consultations
Operations	
Commissioning Development	
Policy	
Human Resources	

Document Purpose	Policy and High Level Procedures
Document Name	Information Sharing Policy – personal information
Publication Date	June 2016
Target Audience	All NHS England staff
Additional Circulation List	n/a
Description	Policy and high level procedures for sharing personal information
Cross Reference	n/a
Superseded Document	n/a
Action Required	To Note
Timing/Deadlines	n/a
Author	Information Governance Taskforce 7E28, Quarry House LEEDS

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

Information Reader Box 3
Document Status 4
1. Introduction 6
2. Scope 7
3. Aims of the policy 7
4. Sharing Information 8
5. Information Sharing Agreements 11
6. Privacy Impact Assessment 13
7. Distribution and Implementation 13
8. Monitoring 14
9. Equality Impact Assessment 14
10. Associated Documents 14
Appendix A: Summary of Legal and NHS Mandated Frameworks 16

1. Introduction

1.1 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.

1.2 The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the Data Protection Act 1998 and the Information Governance Assurance Programme.

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

1.4 An explanation of what is meant by information sharing can be found in section 4.

1.5 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 1998.

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

1.7 In May 2011, the Information Commissioner issued a data sharing code of practice specifying that "under the right circumstances, and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service …. but…. rights under the Data Protection Act must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness."

1.8 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.

1.9 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.

1.10 Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and 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.

1.11 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.

1.12 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

2.1 Staff of the following NHS England areas are within the scope of this document:

- Central Team;
- Regional Teams;
- All Commissioning Support Units;
- Staff working in or on behalf of NHS England (this includes contractors, temporary staff, secondees, all permanent employees and all non-payroll workers).

2.2 Information includes:

- Person identifiable data/information e.g. staff records (see 1.10)
- Personal confidential data - taken from the Caldicott Review, this term describes personal information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

3. Aims of the policy

3.1 The aim of this policy is to:

- Provide a framework for NHS England 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)

- Establish a mechanism for the exchange of information between NHS England and other organisations.

4. Sharing Information

4.1 Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations, or information shared internally within an organisation. Information sharing can take the form of:

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

4.2 Sharing non personal information with other organisations - Key information is shared with other organisations 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.

4.3 Sharing personal information with other organisations – where necessary and proportionate, personal information may be shared with other organisations to: Investigate complaints or potential legal claims; protect children and adults at risk; assess need, service delivery and treatment.

4.3 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.

4.4 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 one-off decisions about sharing.

4.5 '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.

4.6 Ad hoc 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.

4.7 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?** Consider what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the 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?

  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 your local Information Governance team member - https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Lists/Contacts/AllItems.aspx

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

- When information needs to be shared, sharing complies with the law, guidance and best practice;
- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it;
- Individuals' rights will be respected, particularly confidentiality and security
- 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

4.9 Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared. Regard must be had to the document "Anonymisation standard for publishing health and social care data specification"[1] which specifies the steps required to select an appropriate anonymisation plan and to assess re-identification risk (refer to the Information Commissioners Office (ICO) anonymisation code of practice for further information).
http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

[1] http://www.isb.nhs.uk/documents/isb-1523/amd-20-2010/index_html

5. Information Sharing Agreements

5.1 Information sharing agreements – sometimes known as 'Information 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 a data 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.

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

- 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) (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, 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.

5.3 The **Information Governance Toolkit** [2]requirement 207, although not applicable to all organisations but mandatory for the NHS, specifies "When confidential personal information that can identify an individual is shared, both the disclosing and receiving organisations should have procedures that meet the requirements of law and guidance and make clear to staff the appropriate working practices. In some circumstances these procedures (and the law and guidance on which they are based) should be set out within an agreed information sharing agreement or protocol."

[2] The Information Governance Toolkit is a performance tool produced by the Department of Health (DH). It draws together the legal rules and central guidance relating to information governance and presents them in one place as a set of information governance requirements. Organisations are required to carry out self-assessments of their compliance against the IG requirements.

5.4 Requirement 207 goes on to specify that "organisations that are achieving an adequate level of performance (i.e. attainment level 2 or above) against the NHS Operating Framework key IGT 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. Senior personnel in these organisations, e.g. NHS Chief Executives, Directors of Adult Social Services, sign an IG Assurance Statement (formerly an IG Statement of Compliance) to provide the required assurance to partner organisations.

5.5 Therefore, organisations are not required to put in place information sharing protocols where information sharing is between 'trusted organisations' for care purposes. Such protocols may still be of value however where organisations feel that it is important to establish working procedures, contact points etc. that support day to day operational activity.

5.6 Where organisations are unable to demonstrate the required information governance performance to be classified as 'trusted', routine information sharing continues to require information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. This is not to say that these organisations are failing to deliver effective information governance, rather that there is no agreed means for them to demonstrate that they are doing so in the absence of an agreed protocol, e.g. they are not mandated to complete the IG Toolkit."

5.7 **Sharing for Non-care Purposes –** Requirement 207 states that the approach where confidential personal information needs to be shared for non-care purposes needs to be managed somewhat differently even where the sharing is with a 'trusted' organisation (see also IG Toolkit requirement 202). This is because the purposes for sharing need to be defined and limited, and additional requirements such as recorded informed consent or evidence of support under section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001), may be required to enable lawful sharing.

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

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

5.9 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. This agreement covers the sharing of personal identifiable information and explains the process for signing off the agreement.

6. Privacy Impact Assessment

6.1 Before entering into any data sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help to assess the benefits that 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.

6.2 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 privacy impact assessments can be found within the NHS England IG requirements for New Processes, Services, Information Systems and Assets.

6.3 Any new information assets and data flows that arise out of a new project or procurement where NHS England is the data controller or receives personal, confidential, sensitive or business sensitive information will need to be recorded as part of NHS England's wider Information Asset Register. Further information around this can be found at the following intranet location: https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Pages/Information-Asset-Management-.aspx

7. Further advice

7.1 With information sharing there will always be exceptional and difficult circumstances where advice may be needed. The local Caldicott Guardian/Information Governance Specialist should be consulted where there are any concerns about whether the proposed information sharing is appropriate. The Caldicott Guardian 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 Caldicott Log. Please contact you local Information Governance team member around any exceptional needs or requests for information sharing, and any information sharing decisions that may require the Caldicott Guardians input.

8. Distribution and Implementation

8.1 Distribution Plan

8.1.1 This document will be made available to all Staff via the NHS England intranet site.

8.1.2 A global notice will be sent to all Staff notifying them of the release of this document.

8.1.3 A link to this document will be provided from the Information Governance intranet site.

8.2 Training Plan

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

9. Monitoring

9.1 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.

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

10. Equality Impact Assessment

10.1 This document forms part of NHS England'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.

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

11. Associated Documents

11.1 The following documents will provide additional information:

REF NO	DOC REFERENCE NUMBER	TITLE
		Freedom of Information Policy
		Information Governance Policy
		Data Protection Policy
		Document and Records Management Policy
		Information Security Policy
		Confidentiality policy
		Safe Haven Procedure

11.2 External Reference documents

REF NO	ORGANISATION	TITLE	VERSION/ DATE
	Information Commissioners office	Data Sharing: Code of Practice	May 2011
	Health and Social Care Information Centre (HSCIC)	A guide to confidentiality in health and social care: references http://www.hscic.gov.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf	V1.1 – September 2013
	Health and Social Care Information Centre (HSCIC)	Secondary use services: http://www.hscic.gov.uk/susguidance	Multiple guidance documents on web
	Ministry of Justice	Public Sector Data Sharing: Guidance on the Law:http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf	November 2003
	Department of Health	NHS Information Governance:	September

		Guidance on Legal and Professional Obligations	2007
	Department of Health, Social Services and Public Safety http://www.dhsspsni.gov.uk/gmgr-annexe-c8	Common law duty of confidentiality	Undated but as displayed on website as at March 2014
1.0	Information Standards Board	Anonymisation Standard for Publishing Health and Social Care Data Specification (Process Standard)	21/02/13

Appendix A: Summary of Legal and NHS Mandated Frameworks

NHS England 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, who may be held personally accountable for any breaches of information security for which they may be held responsible. NHS England shall comply with the following legislation and guidance as appropriate:

Public Sector Data Sharing: Guidance on the Law

1. 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 is 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 1998
    - the Human Rights Act 1998 and the European Convention on Human Rights;
    - the common law tort of breach of confidence;

2. 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.

3. 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.

4. 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).

5. 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 breaches a duty of confidentiality 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 the local Information Governance Team for further advice and guidance.

6. 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.

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

The Data Protection Act 1998

8. The DPA applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act 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 DPA that are relevant to information sharing are, personal information must be:

    i. Processed fairly[3] 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"
    ii. Processed for specified and lawful purposes.
    iii. Adequate, relevant and not excessive.
    iv. Accurate and where necessary kept up to date.
    v. Not kept longer than necessary, for the purpose(s) it is used.
    vi. Processed in accordance with the rights of the data subject under the Act.
    vii. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
    viii. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

9. The DPA imposes obligations upon 'data controllers' when they are 'processing' 'personal data', and gives rights to 'data subjects'.

10. Sections 1 and 2 of the DPA define these concepts:

    'Data' includes all automatically processed information as well as some manual records

    'Personal data' means data relating to an identified or identifiable living individual. Anonymised data may still be personal data if the data controller can identify who the information relates to.

[3] Personal data are not to be regarded as being processed fairly unless the data subjects are provided with (or have ready access to) certain information, either prior to, or at the time that the processing first takes place, or very soon afterwards. This information includes the identity of the data controller; the purposes for which the data are intended to be processed; and any further information that is necessary in order for the processing to be regarded as fair. Usually this requirement is complied with through the provision of 'fair processing notices' which are drawn to the data subject's attention when they supply the personal data to the data controller.

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

The **'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 persons 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.

Click here for an online link to the Data Protection Act 1998

Human Rights Act 1998

11. 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.

12. 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.

13. 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 DPA, 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 Confidentiality

14. 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.

15. 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.

16. 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.

17. Three circumstances making disclosure of confidential information lawful are:

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

18. 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 should first seek the consent of that patient/client.

19. 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.
20. 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.

21. 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

22. 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.

23. 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.

24. Section 251 was established to enable the common law duty of confidentiality to be overridden 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

25. 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

First published Date
Published to Name, in electronic format only.