hscic Health & Social Care Information Centre

A guide to confidentiality in health and social care: references

Treating confidential information with respect

Version: 1.1

Date: 12 September 2013

Contents

Introduction and how to use this document

This document is the references part of the Guide to Confidentiality in Health and Social Care. It provides some examples of good practice drawn from the relevant principles, obligations and laws outlined in the guide. Throughout the document there are blue boxes highlighting good practice recommended by Dame Fiona Caldicott's Information Governance Review (IGR).

It can be read as stand-alone guidance but would be most useful read as an accompanying document to the Guide to Confidentiality.

The HSCIC has produced both parts of the Guide to Confidentiality under section 265 of the Health and Social Care Act 2012. Therefore any "health or social care body who provides health services, or adult social care in England …(or)…person… who provides health services, or adult social care in England, pursuant to arrangements made with a public body exercising functions in connection with the provision of such services or care must, in providing those services or that care, have regard to the advice or guidance in exercising functions in connection with the provision of health services or of adult social care in England."

This is a living document and will be updated periodically. The first update is due in early 2014 and an accompanying notification and publication process will ensure that version control is effectively managed.

Section 1: The Information Governance Review

The government asked Dame Fiona Caldicott to lead an independent review to see how best to balance the need to keep patient and service user information secure with the need to share it among health and care professionals for legitimate reasons.

The review's report 'Information: to share or not to share?'[1] was published on 26 April 2013.

The review made 26 recommendations which the government has welcomed and accepted in principle. The review's report contains a wealth of helpful detail, but is not itself a legally binding document. Where applicable, the recommendations of the review have been included within this guide.

The good practice guidance in 'Information: to share or not to share?' is laid out in boxes below and should be adopted.

The revised Caldicott principles are also set out below. These principles should underpin information governance across health and social care services.

[1] www.gov.uk/government/publications/the-information-governance-review

The Caldicott principles

1. Justify the purpose(s)

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

2. Don't use personal confidential data unless it is absolutely necessary

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

3. Use the minimum necessary personal confidential data

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

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

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

5. Everyone with access to personal confidential data should be aware of their responsibilities

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

6. Comply with the law

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

7. The duty to share information can be as important as the duty to protect patient confidentiality

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

Section 2: The common law of confidentiality and consent

Common law confidentiality is not codified in an Act of Parliament but built up from case law through individual judgments. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Although judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances. Common law confidentiality can also be overridden or set aside by legislation.

Available guidance on the common law includes the Department of Health (DH) 2003 publication Confidentiality: NHS Code of Practice[2]. However, whilst this remains largely applicable, the guidance has dated and will be superseded in due course by guidance developed under the banner of the Health and Social Care Information Centre (HSCIC)'s 2013 Confidentiality Code of Practice.

Supplementary guidance on the common law, developed by the HSCIC, is provided below after an explanation of consent.

Definitions of consent

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

The Mental Capacity Act 2005 Code of Practice[3] should be consulted with regards to decisions about capacity and competence.

Explicit consent

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

Implied consent

Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses

2 www.systems.hscic.gov.uk/infogov/codes
3 www.justice.gov.uk/downloads/protecting-the-vulnerable/mca/mca-code-practice-0509.pdf

sharing personal confidential data during handovers without asking for the patient's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent.

Duration of consent

Patients can change their consent at any time. Consent is not an open-ended decision. Consent pertaining to the care of a person should be reviewed when any of the following criteria apply:

- The person using the service decides to remove their consent.
- There is a significant change in the person's situation e.g. a new diagnosis and/or a referral.
- After an agreed timescale, which organisations should consider and include as part of their local policies through dialogue with their patients.

The duty of confidence

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is generally accepted that information provided by patients or service users to a health or social care service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. This is an important point, as once information is effectively anonymised it is no longer confidential.

Confidentiality after death

When an individual has died, information relating to that individual remains confidential under the common law (see for example Bluck v The Information Commissioner and Epsom & St Helier University NHS Trust, 2007, Lewis v Redfern Nicholas Lewis (Claimant) v Secretary of State for Health (Defendant) & Michael Redfern QC (Interested Party) [2008] EWHC 2196 (QB), Plon (Societe) v France (Application no 58148/00). Judgment of the Second Chamber of the Strasbourg Court (May 18 2004)).

An ethical obligation to the relatives of the deceased exists and health records of the deceased are public records and governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances. The Access to Health Records Act 1990 permits access to the records of a deceased person by those with a claim arising out of that individual's death. This right of access is negated however if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive). There is no equivalent statutory provision in relation to social care records. Local authorities generally provide access to social care records through the Freedom of Information Act. However, the guidance issued by the ICO on s.41 of the Freedom of Information Act means

relatives could pursue a case for breach of confidence (ICO: Practical guidance: Information about the deceased[4]).

Properly gained consent provides a legal basis for sharing confidential information

When an individual provides consent for sharing information about them for a particular purpose (either for direct care or for other purposes), this consent provides a legal basis for that information sharing. Explicit consent provides a legal defence to potential claims for breach of confidence and breach of privacy; it also ensures that the conditions for processing sensitive personal information in schedules 2 and 3 of the Data Protection Act 1998 are met. Consent may either explicit or, in certain circumstances, implied. Even when consent has been given, this does not mean that information which is unnecessary or irrelevant must be shared.

The individual is usually able to give consent for any information sharing needed to safely provide that care. Very few individuals ever express concern about information sharing where they see it as necessary to provide their care (for 'direct care'). Consent for the necessary sharing of information to support care delivery can be inferred from the fact that an individual agrees to receive that care, however, only relevant information should be shared.

There are three tests for establishing the conditions under which consent can be implied, all of which must be met affirmatively:

- Is the person sharing the information a registered and regulated professional or one of their direct care team?
- Is the activity a type of direct care within the scope specified by the professional's regulatory body?
- Does the professional have a legitimate relationship with the person or persons concerned?

These sit alongside the legal requirements for valid consent.

Sharing common law confidential information without consent for purposes other than direct care

When confidential information is to be used for purposes other than direct care it will usually be shared in a form whereby the individual cannot be identified. If individuals cannot be identified from the information, then consent is not needed.

However, there may be circumstances where it is not practicable to use de-identified information or to get consent and in these cases confidential information may be shared but **only** if there is a legal basis for the information sharing. Note that if an individual objects to sharing, it may be that the confidential information cannot be shared.

4 www.ico.org.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/informationaboutthedeceased.pdf

There are two principal ways that sharing identifiable confidential information may be allowed without consent of the individual:

1. **Statutory or other legal duty mandating sharing:**
   The holder of the confidential information may have a statutory obligation to share or disclose the confidential information or the one seeking to obtain the information may have a statutory basis to demand it. For example, health protection legislation includes a requirement to notify cases of infections or contamination which could present a significant risk to human health. The courts may issue orders that can be challenged but must generally be complied with. A range of bodies have legal authority to obtain confidential information in support of their duties and functions e.g. the Care Quality Commission.

   The HSCIC has statutory authority under the Health and Social Care Act (HSCA) 2012 enabling it to collect information from health and social care organisations. In some circumstances the HSCIC can require organisations to provide information, and in other circumstances it may make non-mandatory requests.

2. **Legal permissions, allowing sharing:**
   Some legislation falls short of creating a duty to share confidential information or a power to collect it though it may make it possible for organisations to share confidential information. This may be in a form that provides a legal gateway to share confidential information where this might otherwise be prevented, or it may simply set the common law obligation of confidentiality aside. Such confidential information sharing must be necessary and proportionate to the purpose.

Example A – Legislation allowing sharing:

Section 251 of the NHS Act 2006: This legislation provides the Secretary of State for Health with the authority to make regulations that set aside legal obligations of confidentiality (though not other legal requirements). Support can be granted for a specific range of activities, for example anonymising information, accessing records to contact people for the purposes of gaining consent for research, geographical analysis, linkage, validation and clinical audit. Further guidance on s.251 and the application process to the Confidentiality Advisory Group (CAG) is available from the Health Research Authority (HRA)[5]. Generally, support is **permissive** i.e. it allows data sharing for the particular purpose, but does not mandate it. Where the Secretary of State is asked to exercise his discretion to approve the release of information he seeks advice from the independent CAG which is hosted by the HRA and makes decisions with respect to research. The Secretary of State will continue to make decisions in relation to all other purposes. In addition, organisations seeking information that might identify individuals for research purposes must have approval from either a local Research Ethics Committee or a multi-centre Research Ethics Committee as appropriate. Guidance on the research governance framework for health and social care[6] is available from the Department of Health. Existing regulations support work related to cancer and to public health risks and surveillance, and provide the Secretary of State with the discretion to support bodies wishing to access identifiable confidential information for other medical purposes, including medical research.

[5] www.hra.nhs.uk/hra-confidentiality-advisory-group/
[6] www.gov.uk/government/publications/research-governance-framework-for-health-and-social-care-second-edition

Example B – The public interest allowing the common law duty of confidentiality to be set aside:

Public interest: This applies when the holder of the information believes that the public good that would be served by sharing the information outweighs both the obligation of confidentiality owed to the individual and the public good of protecting trust in a confidential service. This is a difficult test to satisfy and the circumstances of each individual to whom the information relates need to be considered on a case by case basis. This means that the public interest can rarely provide a legal basis for sharing large volumes of information. Whilst serious crimes such as murder and rape would normally justify sharing with appropriate bodies e.g. the police, there are grey areas where professional experience and judgement are needed and where the circumstances might warrant the sharing of limited information proportionate to the seriousness of the issue.

All processing of confidential information must be lawful. In addition to having one of these legal bases the processing must also meet the requirements of the Data Protection Act and pass the additional tests in the Human Rights Act.

Any processing of confidential information that is not compliant with these laws, even if otherwise compliant with the Data Protection Act, is a data breach, and must be dealt with as such.

When deciding whether to share confidential information, the following should be considered:

- Whether and how individuals should be informed about the information sharing: Individuals must be told, in general terms, which information will be shared with whom, for what purposes and how long it will be held. There are some rare exemptions to this.

- Whether it is necessary to use identifiable information for the specific purpose. The quantity and type of information used must be proportionate to the purpose being addressed and the information should be de-identified as far as is practicable.

- Whether there is any other legal bar to the confidential information sharing.

Many bodies are able to share information, without any particular restriction. However, bodies that have been created under statute are only able to do what they were set up to do, limiting what they might share and with whom they might share it. The law in this area is evolving and becoming less restrictive and statutory bodies will need to obtain legal advice on what they are permitted to do. In some cases Parliament has provided legal authority to organisations to support important work that might need access to information that might identify individuals. This legal authority may enable an organisation to collect information to discharge its functions and the authority may require compliance or might simply remove legal barriers that prevent confidential information from being shared. Legal authority may be given to organisations to act on behalf of others or it may enable one organisation to approve information collection by other organisations. Guidance on the various types of statutory

authority and which bodies may do what is available from the Department of Health (NHS Information Governance Guidance on Legal and Professional Obligations)[7].

[7] systems.hscic.gov.uk/infogov/codes/lglobligat.pdf

Section 3: The Data Protection Act 1998

The Data Protection Act 1998 (DPA) implements the provisions of the EU Data Protection Directive (95/46/EC) and aims to "protect individuals with regard to the processing of personal data and on the free movement of such data".

Schedule 1 of the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA provides a framework that governs the processing of information that identifies living individuals. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers personnel records. The Act also includes other requirements including requirements of notification (formerly registration) with the Information Commissioner, commitment to data quality, effective information security and the extension of a range of rights to service users and patients.

Guidance on the Data Protection Act 1998 is available from the Information Commissioner's Office[8].

The first data protection principle in the Act requires that information is processed lawfully which extends the Act to cover all other legal requirements and restrictions. Guidance on the interaction between the common law duty of confidentiality and the Data Protection Act is provided in the DH publication 'Confidentiality: NHS Code of Practice'.[9]

Fair processing and transparency

The Data Protection Act 1998 requires, as far as is practicable, that individuals are informed about who has access to information that might identify them and for what purposes.

The right to object to confidential information being shared for purposes beyond an individual's care and treatment should be followed through by actual processes to ensure individuals fully understand what they can object to and how to initiate that process, otherwise it could be considered unfair processing.

More information about fair processing is available in the Information Commissioner's Data Sharing Code of Practice[10] and the Information Commissioner's Privacy Notice Code of Practice[11].

[8] www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications
[9] www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf
[10] www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
[11] www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

Section 4: Human Rights Act provisions

Whereas common law confidentiality protects confidential information, the Human Rights Act (HRA)1998 establishes the principle of privacy, conferring rights on individuals to be able to operate without arbitrary interference in their affairs, by incorporating the European Convention on Human Rights (ECHR) into English law.

Article 8(1) of the ECHR states that “Everyone has the right to respect for his private and family life, his home and his correspondence.”

Legislation generally must also be compatible with the HRA 1998, so any proposal for setting aside obligations of confidentiality through legislation must:

a. pursue a legitimate aim;

b. be considered necessary in a democratic society; and

c. be proportionate to the need.

Rights under the HRA 1998 are enforceable against public bodies, such as NHS organisations, and cover health records as these contain private information relating to a person’s health. These rights may be extended to independent sector providers where they provide publicly-funded care through contractual arrangements.

The right to privacy in the ECHR is not absolute, but qualified. Article 8(2) states that there shall be “no interference by a public authority” other than in certain special circumstances, including “for the protection of health”. However, any interference with privacy must meet a “pressing social need”, must be “no greater than is proportionate to the legitimate aim pursued” and must be justified by reasons that are relevant and sufficient for the purpose.

In general, compliance with the Data Protection Act 1998 and the common law of confidentiality will satisfy HRA requirements. However, this is a complex area of law that is open to interpretation by the courts, meaning that specific legal advice should be sought to ensure compliance in the particular circumstances.

Section 5: Professional regulators' guidance

There are eight organisations known as health and social care regulators which oversee one or more of the health and social care professions by regulating individual professionals across the UK. They are listed below and each has specific links to confidentiality guidance. Whilst they may expect practice over and above what is in this guide, it is not expected that any would contradict the practice within this guide.

General Medical Council (GMC)

Doctors

Website: www.gmc-uk.org

Content produced by the GMC in relation to confidentiality includes the GMC's Confidentiality Guidance (2009)[12].

Nursing and Midwifery Council (NMC)

Nurses and midwives

Website: www.nmc-uk.org

Content produced by the NMC in relation to confidentiality includes the NMC's web page on confidential information[13] and sections on confidentiality within The code: Standards of conduct, performance and ethics for nurses and midwives[14].

Health and Care Professions Council (HCPC)

Arts therapists, biomedical scientists, chiropodists / podiatrists, clinical scientists, dieticians, hearing aid dispensers, occupational therapists, operating department practitioners, orthoptists, paramedics, physiotherapists, practitioner psychologists, prosthetists / orthotists, radiographers, social workers in England and speech and language therapists

Website: www.hcpc-uk.org

Content produced by the HCPC in relation to confidentiality includes the HCPC's Confidentiality – guidance for registrants[15].

General Dental Council (GDC)

Dentists, clinical dental technicians, dental hygienists, dental nurses, dental technicians, dental therapists, and orthodontic therapists

Website: www.gdc-uk.org

[12] www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp
[13] www.nmc-uk.org/Nurses-and-midwives/Regulation-in-practice/Regulation-in-Practice-Topics/Confidentiality/
[14] www.nmc-uk.org/Documents/Standards/The-code-A4-20100406.pdf
[15] www.hpc-uk.org/assets/documents/100023F1GuidanceonconfidentialityFINAL.pdf

Content produced by the GDC in relation to confidentiality includes the GDC's Principles of Patient Confidentiality[16].

General Chiropractic Council (GCC)

Chiropractors

Website: www.gcc-uk.org

Content produced by the GCC in relation to confidentiality includes the sections on confidentiality in the GCC's Code of Practice and Standard of Proficiency[17].

General Optical Council (GOC)

Opticians (optometrists and dispensing opticians)

Website: www.optical.org

Content produced by the GOC in relation to confidentiality includes the sections on confidentiality in the GOC's Code of Conduct[18].

General Osteopathic Council (GOsC)

Osteopaths

Website: www.osteopathy.org.uk

Content produced by the GOsC in relation to confidentiality includes the GOsC's Data Protection and Privacy Policy[19].

General Pharmaceutical Council (GPhC)

Pharmacists, pharmacy technicians and pharmacy premises

Website: www.pharmacyregulation.org

Content produced by the GPhC in relation to confidentiality includes the Guidance on Patient Confidentiality[20].

[16] www.gdc-uk.org/Newsandpublications/Publications/Publications/PatientConfidentiality[1].pdf
[17] www.gcc-uk.org/files/link_file/COPSOP_2010.pdf
[18] www.optical.org/goc/filemanager/root/site_assets/publications/codes/codes_of_conduct.pdf
[19] www.osteopathy.org.uk/data-protection/
[20] www.pharmacyregulation.org/sites/default/files/Guidance%20on%20Confidentiality_April%202012.pdf

Examples of guidance on confidentiality and information sharing from regulators

The General Medical Council's advice on good practice that all doctors must follow says:

"Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to seek medical attention or to give doctors the information they need in order to provide good care….But appropriate information sharing is essential to the efficient provision of safe, effective care, both for the individual patient and for the wider community of patients."

The Nursing and Midwifery Council's code says:

"You must respect people's right to confidentiality …You must ensure people are informed about how and why information is shared by those who will be providing their care. You must disclose information if you believe someone may be at risk of harm, in line with the law of the country in which you are practising."

The Health and Care Professions Council oversees standards in 15 health and care professions, including paramedics and social workers.

Its guidance for registrants says:

"Service users expect the health and care professionals involved in their care or who have access to information about them to protect their confidentiality at all times.
This information might include details of a service user's lifestyle, family or medical condition which they want to be kept private. Breaking confidentiality can affect the care or services you provide, as service users will be less likely to provide the information you need to care for them. Doing this may also affect the public's confidence in all health and care professionals."

Section 6: Record-keeping best practice

Record-keeping best practice is outlined in Annex A of the DH publication 'Confidentiality: NHS Code of Practice'[21]. It is covered more generally in the DH publication 'Records Management: NHS Code of Practice: Part 1'[22].

Clinical and corporate information assurance requirements are set out in the Information Governance Toolkit[23].

Data retention standards

All records should be kept in line with health and social care system record retention requirements. Guidance on record retention is provided in the DH publication 'Records Management: NHS Code of Practice: Part 2'.[24]

All patient records held by provider organisations should be kept in line with health and social care system record retention requirements. There are two ways this could be done:

- The provider holding the records could be funded to deliver this retention and security of the records as part of their commissioning contract. If the provider is providing care services they will need to retain the data for a period for their own financial probity and clinical or care governance. If the provider is purely a data processor then they should not need to retain the data beyond the contracted period.
- Another part of the health and social care system, for example the Health and Social Care Information Centre, could be commissioned to provide a 'safe vault' for this data which can only be accessed when there is anonymisation at source, or when there is complaint, legal challenge or criminal investigation.

[21] www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf
[22] webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747
[23] nww.igt.connectingforhealth.nhs.uk/
[24] webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Section 7: Sharing information for direct care

Health and social care providers should audit their services against NICE Clinical Guideline 138[25], specifically against those quality statements concerned with sharing information for direct care.

Registered and regulated professionals

Confidential information needs to be shared between registered and regulated health and social care professionals who have a legitimate relationship with the individual for the purposes of the individual's direct care. A registered and regulated health or social care professional has a legitimate relationship with the patient or service user when any or all of the following criteria are met:

- The individual presents themselves to the professional to receive care.
- The individual agrees to a referral from one care professional to another.
- The individual is invited by a professional to take part in a screening or immunisation programme for which they are eligible and they accept.
- The individual presents to a health or social care professional in an emergency situation where consent is not possible.
- The relationship is part of a legal duty e.g. contact tracing in public health.
- The individual is told of a proposed communication and does not object e.g. the consultant in the ambulatory clinic says she will let the patient's social worker know of events in the clinic and the patient does not object.

[25] www.nice.org.uk/cg138

Non-regulated staff providing direct care

When providing direct care, a non-regulated member of staff should be able to access a proportion of an individual's confidential information when any or all of the following criteria are met:

- The individual presents themselves to those staff for the purposes of care e.g. NHS 111.
- The staff are professionally supervised by a registered and regulated health or social care professional.
- The staff are managerially directly responsible to a registered and regulated professional for the lawful use of confidential information.
- They have only necessary and very limited access to patient and service user data.
- The individual concerned has given explicit consent that the member of staff should access all or part of their confidential information.
- The staff member is registered on a voluntary register approved by the Professional Standards Authority.

And in all cases:

- The terms and contractual obligations of employment within an organisation have an explicit duty of confidentiality as part of the contract with sanctions.
- The non-regulated individual is a part of a direct care team with a 'legitimate relationship' to the individual.

Communication between regulated and non-regulated staff

Appropriate communication from a regulated and registered professional to non-regulated staff should be the norm and occur through one of the following routes:

- The individual concerned gives explicit consent to the sharing of their confidential information.
- The contact point of the service is a registered and regulated health and social care professional and communication is through implied consent.
- The communication is through the social worker or equivalent professional within the local authority who has organised the package of care ('care and support plan').
- The communication is given to the individual concerned, with or without a carer being present, and the individual makes the decision to share their copy of the communication.
- There is a specific safety concern regarding the individual, which is best resolved or mitigated by sharing some of the confidential information about the patient in situations where consent is not possible. In these situations, professional judgement and the patient's best interests need to apply.

Mental and sexual health information

Of course, careful judgment is required when sharing highly sensitive information. Information about mental health and sexual health is widely recognised to be some of the most sensitive that is recorded within care records.

The Royal College of Psychiatrists has provided the following guidance on Good Psychiatric Practice: Confidentiality and Information Sharing[26] which considers issues in relation to mental health.

General guidance on both mental health and sexual health aspects of information sharing are provided in the DH publication Confidentiality: NHS Code of Practice.[27]

[26] www.rcpsych.ac.uk/files/pdfversion/cr160.pdf
[27] www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf

Section 8: Carers, family members and friends

Those involved in the direct care of a patient/service user should establish with them what information they wish to be shared, with whom, and in what circumstances. This will be particularly important if the patient has fluctuating or diminished capacity or is likely to lose capacity, even temporarily. Early discussions of this nature can help to avoid disclosures to which patients would object. They can also help to avoid misunderstandings with, or causing offence to, anyone with whom the patient/service user would want information to be shared.

Some friends and/or family have a special relationship with the patient/service user in that they act as a carer. Confidential information should be shared with the carer, when the patient/service user has given explicit, informed consent. In circumstances where the patient/service user cannot give valid consent, confidential information should be shared with the carer subject to open dialogue with the patient if possible. If it is not possible to engage in open dialogue, information should be shared with the carer in the incapacitated person's best interests, when ALL the following criteria are met:

- the patient/service user lacks capacity;
- the carer 'cares for' the patient/service user;
- there is no legal documentation in place to prevent sharing;
- there are no contra-indications to sharing in the patient's/service users' record; and
- there are no safeguarding issues apparent.

Hearing the concerns of and gaining information from third parties

If anyone close to the patient/service user wants to discuss their concerns about the patient's/service user's health, health and care staff should make it clear to them that, while it is not a breach of confidentiality to listen to their concerns, they cannot guarantee that they will not tell the patient/service user about the conversation. Health and care staff might need to share with a patient/service user information they have received from others, for example, if it has influenced their assessment and treatment of the patient/service user. Health and care staff should not refuse to listen to a patient's/service user's partner, carers or others on the basis of confidentiality as the information they provide might be helpful in the health or care staff's care of the patient. At the same time staff will need to be alert to bias, malice or simple misconceptions.

There are occasions when a third party, such as a family member, offers information to a registered and regulated professional who is part of an individual's care team when the patient/service user is absent. The professional should explain to the third party that either at the time or sometime in the future the patient/service user may be able to identify the source of the information even if the identity of the third party is withheld. This should be undertaken BEFORE the third party has disclosed the information they wish to share. This means the third party has the following options:

- The third party consents to the patient/service user finding out their identity.
- The third party wants the information recorded and understands there is a residual risk of them being identified as the source of the information even if it is not readily identified to the patient/service user by patient online access.
- The third party decides NOT to tell the professional the things they were planning to. (This is only possible if the information about the patient/service user has not already been disclosed.)

Sharing genetic or similar information with family members

Genetic and some other information about the patient might also be information about others with whom the patient shares genetic or other links. The diagnosis of an illness in the patient might, for example, point to the certainty or likelihood of the same illness in a blood relative.

Most patients will readily share information about their own health with their children and other relatives, particularly if they are advised that it might help those relatives to:

- get prophylaxis or other preventative treatments or interventions;
- make use of increased surveillance or other investigations, or
- prepare for potential health problems.

However, a patient might refuse to consent to the disclosure of information that would benefit others, for example where family relationships have broken down, or if their natural children have been adopted. In these circumstances, disclosure might still be justified in the public interest. If a patient refuses consent to disclosure, health and care staff will need to balance their duty to make the care of the patient their first concern against their duty to help protect the other person from serious harm. If practicable, health and care staff should not disclose the patient's identity in contacting and advising others of the risks they face.

The information governance principles for providing direct care for patients with genetic conditions are exactly the same as the direct care of any patients. However, there is a particular challenge with regard to the creation of a legitimate relationship between a geneticist and a family member. This often involves complex practices, including consent forms, which do not arise in other areas of health and social care.

Either of the following solutions are appropriate in creating a legitimate relationship:

- The geneticist gives the patient a letter of explanation for their family members on why they should seek the attention of a geneticist either directly or through their general practitioner which the patient then shares with his or her family members.

- The patient agrees to the disclosure of some of their confidential information to their family, and after getting the agreement of family members discloses to the geneticist the contact details of those family members. The geneticist contacts the family members disclosing the issues agreed with the patient and advises the family member on contacting the genetics service and/or their GP for advice.

In some rare cases the patient's consent may be overruled if disclosure of data is sufficiently in the public interest, i.e. not disclosing data will result in someone suffering significant harm.

Section 9: Safeguarding

Safeguarding children

The action taken to promote the welfare of children and protect them from harm is everyone's responsibility. Everyone who comes into contact with children and families has a role to play.

Safeguarding and promoting the welfare of children can be defined as:

- protecting children from maltreatment;
- preventing impairment of children's health or development;
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- taking action to enable all children to have the best outcomes.

Children are best protected when professionals are clear about what is required of them individually, and how they need to work together.

For further details see the DH guidance on Working Together to Safeguard Children[28].

Safeguarding vulnerable adults

A 'vulnerable adult' is a person:

- who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or may be unable to take care of him or herself.
- or unable to protect him or herself against significant harm or exploitation.

For further details see DH guidance on multi-agency working to safeguard vulnerable adults: No secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse[29].

Domestic violence

It should be noted that in cases involving domestic abuse, for example, the victim may be placed at risk if confidential information about her or him is inadvertently shared.

Questions from an apparently concerned partner may seem to be innocent, but answering them may help the partner to find the victim, who may then be re-victimised or even murdered.

[28] www.education.gov.uk/aboutdfe/statutory/g00213160/working-together-to-safeguard-children
[29] www.gov.uk/government/uploads/system/uploads/attachment_data/file/194272/No_secrets__guidance_on_developing_and_implementing_multi-agency_policies_and_procedures_to_protect_vulnerable_adults_from_abuse.pdf

Knowing that a patient is being subjected to violence or abuse, which is serious in nature, may be sufficient to trigger sharing in the public interest.

For further guidance see the guidance on multi-agency risk assessment conferences in cases of domestic violence: Striking the Balance: Practical Guidance on the Application of Caldicott Guardian Principles to Domestic Violence and MARACs (Multi Agency Risk Assessment Conferences). [30]

[30] www.gov.uk/government/uploads/system/uploads/attachment_data/file/146730/dh_133594.pdf.pdf

Section 10: Using health and social care information – direct care and indirect care purposes

The Guide to Confidentiality distinguishes between information that is used for direct care and information that is used for purposes other than care (indirect care).

Direct care

The term ‘direct care’ is defined as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual). It includes:

- supporting individuals’ ability to function and improve their participation in life and society;
- the local audit/assurance of the quality of care provided;
- the management of untoward or adverse incidents;
- the measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

It does not include research, teaching, financial audit, service management activities or risk stratification (see note below on borderline cases).

The direct care team

Sharing for direct care can take place across departmental and organisational boundaries. For example, the direct care team may include physiotherapists, nurses, midwives, occupational therapists and others on regulated professional registers. For direct care of an individual, registered and regulated social workers must also be considered part of the care team and covered by implied consent when the social worker has a legitimate relationship to the individual concerned.

Indirect care

The term ‘indirect care’ is defined as activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of indirect care activities include risk prediction and stratification (see note below on borderline cases), service evaluation, needs assessment, and financial audit.

The key reason for distinguishing between purposes in this way is that it is generally possible to imply consent for the use of confidential information for direct care purposes but not for

other purposes. There are some exceptions and some tricky borderline cases on which specific guidance is provided.

The searching of patient or service user records for potential research subjects can be done legally by fulfilling any of the following criteria:

- The researcher gains the explicit consent of every patient with a record in the population pool being assessed.
- The search is conducted by a health or social care professional who has a 'legitimate relationship' with the patient, such as a clinician or social worker (see section 3.6 of the Information Governance Review).
- The search is conducted by a researcher who is part of the clinical team.
- The search makes use of 'privacy enhancing technologies'.
- Support under section 251 regulations is granted for the research.

Exceptions

The main exception relates to essential activity that aims to quality assure the care that has been provided. People receiving care should understand that, for their own safety and to improve care provided to others in the future, it is essential that their records are checked. This helps to ensure that the care they received was optimal and that lessons can be learned where necessary. It is generally accepted that consent can be implied for activity concerned with the quality assurance of care, but only when the audit is undertaken by those who are part of the direct care team. An argument could be made that this activity is sufficiently in the public interest that the duty of confidentiality can be overridden. When exceptionally, an individual has objected to records being looked at for these purposes, this should be respected unless there are such strong concerns about the care that has been provided that the public interest must take priority.

Borderline cases

Some activities can appear to sit within a grey area where the relationship of the activity to direct care is not clear.

An important activity that some feel falls within this borderline is that of risk stratification, also known as predictive risk modeling, where records are reviewed to establish a cohort who might then be invited to receive a particular type of care or intervention. However, whilst this activity might eventually result in direct care being provided to a sub-set of those whose records are reviewed, the risk stratification stage falls into one of two separate categories:

1. Rare cases, where professionals have access to confidential information to make decisions about their own patient/service user, which can be done on the basis of implied consent as it is considered to be direct care.

2. When commissioning organisations (e.g. Clinical Commissioning Groups) are making commissioning decisions, which is indirect care and so requires explicit consent or a legal basis.

NHS England guidance on how to lawfully conduct risk stratification is available: Information Governance and Risk Stratification: Advice and Options for CCGs and GPs[31].

Early intervention/help

The Information Governance Review concluded that from an information governance perspective there is a need to ensure that the process of identifying individuals or groups of people for early intervention or help (as well as the interventions themselves) is properly underpinned by meeting all the following criteria:

- There is a basis in law for processing the confidential information.
- There are appropriate approaches to linking data (see sections 3.14, 6.3, 6.5 and 12.6 of the Information Governance Review).
- There are appropriate contractual arrangements in place to process de-identified data for limited disclosure or limited access (see sections 6.3, 6.5 and 12.10 and appendix 6 of the Information Governance Review).
- If help is to be offered, a clear legitimate relationship should exist between the individual or family identified and the person making contact with them (see section 3.6 of the Information Governance Review).

Sharing and risk assessment

Any organisation deciding whether to share information or not should first consider three key questions:

- What is the purpose of the information sharing — is there a clear objective that can best be achieved by sharing the information?
- What is the risk to individuals (both the subject of the information or any third parties) of sharing the information and is this risk proportionate to the benefits to the individual that will be achieved? This includes considering if there is a risk to individuals if the information is not shared.
- How will the information be shared?

[31] www.england.nhs.uk/wp-content/uploads/2013/06/ig-risk-ccg-gp.pdf

Section 11: Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. They help to:

- identify privacy risks to individuals;
- identify confidentiality, privacy and Data Protection compliance liabilities for an organisation;
- protect an organisation's reputation;
- instil public trust and confidence in an organisation's project/product;
- avoid expensive, inadequate "bolt- on" solutions;
- inform an organisation's communications strategy; and
- represent enlightened self-interest.

PIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed;
- organisations know what they want to do;
- organisations know how they want to do it;
- and organisations know who else is involved.

But ideally they should be started before:

- decisions are set in stone;
- organisations have procured systems;
- organisations have signed contracts, Memorandum Of Understandings (MOUs) or agreements; and
- while organisations can still change their mind.

Guidance on Privacy Impact Assessments (Privacy Impact Assessments – An Overview[32]) is provided by the Information Commissioner.

[32] www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW.ashx

Section 12: Anonymisation guidance

There are various technical processes that can be used to transform data to make it less likely that individuals can be identified. It must be stressed that:

- the use of any particular technique does not guarantee "anonymity" of the data; and
- the extent to which data are effectively anonymised is context-dependent.

Techniques may reduce the risk of identification, but there must be a separate assessment of whether the reduced risk is acceptable in particular circumstances and whether the technical process constitutes "effective anonymisation" if this is required.

It should also be noted that even where it is legally permissible to use person identifiable information, its use should be minimised, for example by only sending a relevant subset of the information, or by the use of one or more of the techniques described in guidance.

The Information Standards Board (ISB) Anonymisation Standard[33] outlines techniques on making data less identifiable and on when it is safe to publish data and disclose information for Freedom of Information purposes.

The Information Commissioner has published the Anonymisation: managing data protection risk code of practice[34].

The Office of National Statistics has published statistical guidance and methodology[35].

[33] www.isb.nhs.uk/library/standard/128
[34] ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx
[35] www.ons.gov.uk/ons/guide-method/index.html

Section 13: Accredited Safe Havens

An Accredited Safe Haven (ASH) is an accredited organisation, or a designated part of an organisation, which is contractually and legally bound to process data in ways that prevent the identity of individuals to whom the data relates from being identified. As part of new accountability arrangements across the new health and care system in England, a specific group has been established to consider information governance issues. One of the options that will be considered by this group (the Information Services Commissioning Group (ISCG) Information Governance Subgroup) is the establishment of accredited safe havens as suggested by the Information Governance Review.

Data stewardship requirements for accredited safe havens

Accredited Safe Havens should be required to meet the following requirements for data stewardship:

- Attributing explicit responsibility for authorising and overseeing the anonymisation process e.g. through a Senior Information Risk Officer.
- Appropriate techniques for de-identification of data, the use of 'privacy enhancing technologies' and re-identification risk management.
- The use of 'fair processing notices'.
- A published register of data flowing into or out of the safe haven including a register of all data sets held.
- Robust governance arrangements that include, but are not limited to, policies on ethics, technical competence, publication, limited disclosure/access, regular review process and a business continuity plan including disaster recovery.
- Clear conditions for hosting researchers and other investigators who wish to use the safe haven.
- Clear operational control including human resources procedures for information governance, use of role-based access controls, confidentiality clauses in job descriptions, effective education and training and contracts.
- Achieving a standard for information security commensurate with ISO2700 and the Information Governance Toolkit.
- Clear policies for the proportionate use of data including competency at undertaking privacy impact assessments and risk and benefit analysis.
- Standards that are auditable.
- A standard template for data sharing agreements and other contracts that conforms to legal and statutory processes.
- Appropriate knowledge management including awareness of any changes in the law and a joined-up approach with others working in the same domain.
- Explicit standard timescales for keeping data sets including those that have been linked, which should be able to support both cohort studies and simple 'one-off' requests for linkage.

Section 14: Data sharing contracts and agreements

Even between public bodies, there should be information sharing contracts in place that make clear the information governance arrangements that must be in place for each party. The HSCIC Data Sharing Contract[36] provides an example.

Some circumstances require a data sharing contract and these are between a data controller and data processor or an Accredited Safe Haven (see Section 13).

Other circumstances will require a data sharing agreement, for example in data controller to data controller disclosures where there is a lawful basis for disclosure.

There may be circumstances where a data controller wishes to control how a recipient data controller may use the data, in which case a contract may be appropriate with penalties for failure to comply with the requirements.

[36] www.hscic.gov.uk/confguideorg

Section 15: The Health and Social Care Information Centre's powers under the Health and Social Care Act 2012

HSCIC powers to collect information

The HSCIC may establish systems to collect and analyse health and social care information where directed or requested to do so. Collection under directions from the Secretary of State (SoS) or NHS England must be complied with. Similarly, requests from Monitor, CQC and NICE (known as principal bodies) also require the information from providers. These requests are known as mandatory requests.

Other bodies and organisations, including devolved administrations, may request information from providers. These are known as non-mandatory requests.

In all cases, the body asking the HSCIC to establish the information system must consult with the HSCIC in advance. Unless otherwise directed, the HSCIC has discretion in complying with non-mandatory requests. The HSCIC may refuse a request if it interferes to an unreasonable extent with the HSCIC's core functions, if it is not compliant with the Code of Practice for Confidential Information, or if the requestor has ignored the HSCIC's advice on the collection as described below. The HSCIC must comply with a mandatory request unless it relates to information prescribed in regulations.

Also the SoS or NHS England may direct the HSCIC not to comply with non-mandatory requests made by any organisation and may direct the HSCIC to comply with a request from an organisation outside England. The HSCIC does not have the power to refuse a direction from the SoS or NHS England.

The HSCIC may charge a reasonable fee for complying with directions from NHS England or requests from others.

Procedures for assessing collection requests

The HSCIC is required to consult with relevant organisations (requestor and users of the data) before setting up a new collection. The HSCIC will publish procedures for assessing each collection request with the requestor and those that will be required to submit the data. The process will include consideration of any appeals against decisions not to comply with a collection request.

The HSCIC will keep a register and publish details of all collection requests it is obliged to or decides to comply with. It will also maintain a list of requests that have been refused with details of the reasons for refusal.

Providing advice on data collections

The HSCIC may advise any organisation (not just those directing or requesting the HSCIC to collect data) on issues relating to the collection, analysis, publication or other dissemination

of information and may be required to provide such advice by the SoS or NHS England. All persons must have due regard to this advice.

The SoS must request the HSCIC's advice on how the burdens relating to the collection of information imposed on health or social care bodies and other persons may be minimised at least once every three years.

The HSCIC has the power to require health and social care bodies (and those commissioned to provide health and social care services in England) to provide it with the information it needs for the directions and requests described above. Organisations must provide information to the HSCIC in the form and frequency specified by the HSCIC. The HSCIC can request that other organisations (i.e. those not providing 'NHS' commissioned health and adult social care) provide the information, but these organisations do not have to comply.

The HSCA 2012 provides the power for the HSCIC to collect confidential information under a variety of circumstances. The HSCA 2012 states that in providing confidential information to the HSCIC, the provider is not breaching common law confidentiality, but this does not set aside restrictions of any other Act, e.g. DPA, Human Fertilisation and Embryology Act 1990 (HFEA), etc.

The HSCIC can require health and social care bodies to provide confidential information needed to comply with directions from the SoS/NHS England, or to comply with mandatory requests.

Additionally, the HSCIC can collect confidential information for non-mandatory requests, but only if the requestor has the legal right to ask for it, e.g.:

- Where the requestors can require the data to be disclosed to themselves or the HSCIC (for example, under other regulations); or
- Where the data can otherwise lawfully be disclosed to the requestor or the HSCIC (for example, through s.251 support); or
- Where there is documented evidence that the consent of the data subjects has been obtained.

The HSCIC may pay providers commissioned to provide health and social care services to provide confidential information that has been requested.

The HSCIC will publish a procedure to notify organisations of the requirements and requests for information. When identifying information collection requirements, the HSCIC is required to cooperate with others that might be requesting the same information to avoid duplication of effort and to minimise the burden on information providers.

Release of information from the HSCIC

Unless directed otherwise by the SoS or NHS England, the HSCIC must publish (in the public domain) data it collects or derives through analysis unless the data identifies the individual to whom the data relates or it enables their identity to be established.

Information may be published where it identifies a relevant person (that is a health or adult social care provider or organisation) and the HSCIC considers it is in the public interest to do

so. The SoS or NHS England may oblige the HSCIC to publish such information within their directions.

Data must not be published if the HSCIC believes it does not meet the required information standards or it would not be in the public interest to publish it.

Any direction or request to establish an information system may specify when and in what format the information is to be published and the HSCIC must adhere to this.

When publishing information, the HSCIC must consider the need to make it easily accessible for those likely to require access and for the purposes it may be used for.

Dissemination of information (sharing with a specific person or body)

The HSCIC may disseminate information (i.e. share it with a specific person or body rather than publishing in the public domain) that it collects as a result of a direction or a request if it:

- Is in a non-identifiable form; or
- Identifies a relevant person (provider of health care or adult social care or a body corporate) or enables their identity to be ascertained and consent for dissemination has been obtained or the HSCIC considers it appropriate given the public interest vs. the interest of the relevant person; or
- Is identifiable or enables an individual's identity to be ascertained and consent for dissemination has been obtained;
- The information is not being published only because it does not meet the appropriate standards (i.e. is not of good quality) but it is in the public interest to disseminate it; or
- The direction from SoS or NHS England prohibits publication but requires dissemination and there is no other barrier to publication.

The HSCIC may also disseminate information it collects to any organisation where the organisation submitting it to the HSCIC could have lawfully disclosed it directly.

The HSCIC may disclose information (including confidential information) where there is a lawful basis to do so, for example:

- Where that data has been previously lawfully disclosed to the public;
- In accordance with a court order;
- Where it is expedient to protect the welfare of an individual (but common law still applies);
- To another organisation that requires the information to exercise their functions under the provisions of this or of any other Act (but common law still applies);
- In the investigation of a criminal offence (but common law still applies);

- For the purpose of criminal proceedings whether or not it is within the UK;
- Further to s.251 approval;
- If otherwise lawfully allowed.

Data retention

The HSCIC can destroy data it has collected or derived from a collection when it is no longer needed.

Section 16: Legislation that controls confidential information disclosures

There is a wide range of legislation that impacts upon the way that information is used and shared. This is clearly an evolving picture and the HSCIC will endeavour to maintain an up-to-date reference guide. At the present time the most complete guide is the DH publication: NHS Information Governance Guidance on Legal and Professional Obligations.[37]

Whilst this guidance covers a large proportion of the legislation that controls information disclosure, for specialist areas not covered in this guidance, organisations should seek legal advice.

Section 251 of the NHS Act 2006 support

A specific example of legislation that controls confidential information disclosures is Section 251 of the NHS Act 2006 which allows sharing of confidential information in the 'public interest.' It sets a high threshold (but lower than the public interest test) before the duty of confidentiality can be set aside for the purposes of research, audit and other important activities not directly associated with care.

This application process is very rigorous and is managed by the Confidentiality Advisory Committee (CAG). Applicants must demonstrate that the aim of the processing is in the public interest, that anonymised information could not be used to achieve the required results, and that it would be impractical - both in terms of feasibility and appropriateness - to seek specific consent from each individual affected. For research, the approval of a Research Ethics Committee is also needed. The test is one of necessity, not convenience.

The powers under the section 251 regulations only provide relief from the common law duty of confidence. Any activity taking place with the support of section 251 must still comply in full with the Data Protection Act. For example, there must be a clear purpose rather than a fishing expedition for what can be found. The CAG also needs to be certain that appropriate processes are in place to ensure the confidential information is handled responsibly and securely.

[37] systems.hscic.gov.uk/infogov/codes/lglobligat.pdf

Section 17: Information security management

Information security is essential for all types of confidential records, whether manual or electronic. Organisations must ensure staff take basic precautions against information security breaches, such as not leaving portable computers, medical notes or files in unattended cars or in easily accessible areas. All files and portable equipment should be stored under lock and key when not actually being used. Staff should not normally take patient/service user records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed.

Guidance on information security is provided in the DH publication 'Information Security: NHS Code of Practice'[38].

Detailed information security assurance requirements are set out in the Information Governance Toolkit.[39]

[38] www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securitycode.pdf
[39] nww.igt.connectingforhealth.nhs.uk/

Section 18: Objections to sharing

The NHS Constitution[40] states that individuals have the right to object to information about them being shared in a form that might identify them and in general to have reasonable objections to this sharing upheld. This is a broad statement that reflects the more complex legal framework.

The process for considering objections should:

- explicitly include the most senior registered and regulated health and social care professional caring for that individual;
- explicitly include in the consideration whether not supporting the objection will damage the effectiveness of care;
- explicitly include whether there is a demonstrable risk that the safety of the patient will be reduced by not upholding the objection; and
- explicitly include whether there are compelling legitimate grounds relating to the individual's situation.

The Data Protection Act 1998 provides a basis for individuals to raise objections to the sharing of personal data, (i.e. data that identifies or might enable them to be identified in the circumstances) where they feel that they are suffering or may suffer significant harm or distress as a result. The data controller considering the objection might voluntarily choose to stop processing data about the individual concerned but must otherwise consider whether or not the processing is justified despite the individual's claim of harm or distress. If the objection is not sustained then the individual may appeal to the courts. Data that is processed under statute is exempt from these provisions.

The common law of confidentiality provides a basis for individuals to express a preference about the sharing of information that they provided in circumstances where it was reasonable to assume that the information concerned was subject to the common law provisions. In the absence of consent, information held in confidence may only be shared when there is a statutory basis or a public interest justification that outweighs the obligation of confidentiality.

S251 NHS Act 2006 provides a basis, through regulations, for setting the common law confidentiality requirements aside, generally replacing them with approvals or other conditions. Whilst it would be possible to use the power provided to override patient objections in emergencies, this has never been invoked and support under the current regulations is generally provided under a condition that objections are respected.

The Human Rights Act (Article 8 of the European Convention on Human Rights) requires reasonable objections to the disclosure of personal confidential data to be respected.

The Health and Social Care Act 2012 provides a basis for the Health and Social Care Information Centre to collect information that is held in confidence when directed or

[40] www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf

requested to collect the information by the bodies listed in the legislation. NHS England and the Secretary of State may direct the HSCIC to collect information and NICE, Monitor and the Care Quality Commission may request that it do so. However, these bodies have agreed that, in the absence of an emergency or exceptional public interest grounds, they will limit directions and requests to information where an individual has not raised an objection, thus providing individuals with a means of preventing their data being collected in an identifiable form.

To ensure that individuals fully understand what they can object to and how to initiate that process it is important that Data Controllers, such as GPs, act upon the fair processing and transparency requirements outlined by the Data Protection Act (See section 3 above, in particular the Information Commissioner's Privacy Notice Code of Practice[41]).

[41] www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

List of key documents

The following is a list of key documents which underpin much of the guidance within this guide but which are not covered in detail elsewhere. This list will be amended and added to as this 'living' document evolves:

The NHS Constitution

Relevant parts of the NHS Constitution include:

Patients and the public – your rights and NHS pledges to you

You have the right of access to your own health records.

You have the right to be informed about how your information is used.

You have the right to request that your confidential data is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

The NHS also commits:

- to ensure those involved in your care and treatment have access to your health data so they can care for you safely and effectively (pledge).
- to anonymise the data collected during the course of your treatment and use it to support research and improve care for others (pledge).
- where identifiable data has to be used, to give you the chance to object wherever possible (pledge).
- to inform you of research studies in which you may be eligible to participate (pledge).
- to share with you any correspondence sent between clinicians about your care (pledge).
- to offer you easily accessible, reliable and relevant information **and support to use it**. This will enable you to participate fully in your own healthcare decisions and to support you in making choices. This will include information on the range and quality of clinical services where there is robust and accurate information available (pledge).
- to provide you with the information and support you need to influence and scrutinise the planning and delivery of NHS services (pledge).
- to involve you in discussions about planning your care and to offer you a written record of what is agreed if you want one (pledge).
- to encourage and welcome feedback on your health and care experiences and use this to improve services (pledge).

Staff - your responsibilities

You have a duty to protect the confidentiality of personal information that you hold.

You should aim:

- to inform patients about the use of their confidential data and to record their objections, consent or dissent; and
- to provide access to a patient's data to other relevant professionals, always doing so securely, and only where there is a legal and appropriate basis to do so.

Care Record Guarantees

Two Care Record Guarantees for England were developed by the National Information Governance Board (NIGB) which no longer exists. One was designed for the NHS[42] and one for social care[43]. They set the rules that govern how patient and service user information is used in the NHS and social care and what control the patient or service user can have over this. The advice is based on professional guidelines, best practice and the law and applies to both paper and electronic records.

The NHS and Social Care Record Guarantees include information on:

- people's access to their own records,
- how access to an individual's healthcare record will be monitored and policed and what controls are in place to prevent unauthorised access,
- options people have to further limit access,
- access in an emergency,
- what happens when someone is unable to make decisions for themselves.

[42] www.nigb.nhs.uk/pubs/nhscrg.pdf
[43] www.nigb.nhs.uk/bookletlr.pdf

Glossary

Aggregate(d) data/information: Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

Anonymisation: The process of rendering data into a form which does not identify individuals and where there is little or no risk of identification (identification is not likely to take place).

Audit: An audit is an official internal or external examination of an organisation. See 'Clinical audit' and 'Independent audit'.

Caldicott Guardian: A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.

Care pathway: A care pathway is anticipated care placed in an appropriate time frame, written and agreed by a multi-disciplinary team. It has locally agreed standards based on evidence, where available, to help a patient with a specific condition or diagnosis move progressively through the clinical treatment.

Carer: An individual who provides unpaid care to a patient or service user, most commonly a member of their family or friend. For paid workers, the term 'care worker' should be used.

Care records: Care records are personal records. They comprise documentary and other records concerning an individual (whether living or dead) who can be identified from them and relating:

- to the individual's physical or mental health;
- to spiritual counselling or assistance given or to be given to the individual; or
- to counselling or assistance given or to be given to the individual, for the purposes of their personal welfare, by any voluntary organisation or by any individual who:
    - by reason of the individual's office or occupation has responsibilities for their personal welfare; or
    - by an order of a court has responsibilities for the individual's supervision.

This record may be held electronically or in a paper file or a combination of both.

Care team: The health and/or social care professionals and staff that directly provide or support care to an individual.

Children and young persons (or young people): People under 18.

Clinical audit: Clinical audit is a tool for improving practice, patient care or services provided. It is used to measure current practice and care against a set of explicit standards or criteria, identify areas for improvement, make changes to practice and re-audit to ensure that improvement has been achieved. The findings of the clinical audit provide evidence of the quality of practice and care.

Commissioning (and commissioners): Commissioning is essentially buying care in line with available resources to ensure that services meet the needs of the population. The process of commissioning includes assessing the needs of the population, selecting service providers and ensuring that these services are safe, effective, people-centred and of high quality. Commissioners are responsible for commissioning services.

Confidential data or information: See 'Personal confidential data'.

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

Data: Qualitative or quantitative statements or numbers that are (or are assumed to be) factual. Data may be raw or primary data (e.g. direct from measurement), or derivative of primary data, but are not yet the product of analysis or interpretation other than calculation.

Data breach: Any failure to meet the requirements of the Data Protection Act, unlawful disclosure or misuse of personal confidential data and an inappropriate invasion of people's privacy.

Data controller: A person (individual or organisation) who determines the purposes for which and the manner in which any personal confidential data are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA.

Data loss: A breach of principle 7 of the DPA or an inappropriate breaking of confidentiality.

Data processor: In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors are not directly subject to the Data Protection Act. But the Information Commissioner recommends that organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing and a written contract (detailing the information governance requirements) must be in place to ensure compliance with principle 7 of the Data Protection Act.

De-identified: Information which identifies an individual has been removed, but there is still some risk of re-identification.

Direct care: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

Genetic information: Genetic information is information about the genotype, or heritable characteristics of individuals obtained by direct analysis of DNA, or by other biochemical testing. Genetic information in itself is not always identifiable.

Health or Social Care Body: A public body which exercises functions in connection with the provision of health services or of adult social care in England.

Identifiable information: See 'Personal confidential data'.

Identifier: An item of data, which by itself or in combination with other identifiers enables an individual to be identified. Examples include:

1. Names.

2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, postcode, and their equivalent geographical codes, except for the initial four digits of a postcode if, according to the current publicly available data from the Office for National Statistics and/or the Information Commissioner's Office:

a. The geographic unit formed by combining all postcodes with the same four initial digits contains more than 20,000 people.

b. The initial three digits of a postcode for all such geographic units containing 20,000 or fewer people are changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

4. Telephone numbers.

5. Facsimile numbers.

6. Electronic mail addresses.

7. National Insurance numbers.

8. NHS number and medical record numbers.

9. Health plan beneficiary numbers.

10. Account numbers.

11. Certificate/licence numbers.

12. Vehicle identifiers and serial numbers, including licence plate numbers.

13. Device identifiers and serial numbers.

14. Web universal resource locators (URLs).

15. Internet protocol (IP) address numbers.

16. Biometric identifiers, including fingerprints and voiceprints.

17. Full-face photographic images and any comparable images.

18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Information Commissioner's Office.

Independent audit: An audit conducted by an external and therefore independent auditor to provide greater public assurance. See 'Audit' and 'Clinical audit'.

Indirect care: Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research.

Information: Information is the "output of some process that summarises, interprets or otherwise represents data to convey meaning." Data becomes information when it is combined in ways that have the potential to reveal patterns in the phenomenon.

Information governance: How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

Legitimate relationship: The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care.

Linkage: The merging of information or data from two or more sources with the object of consolidating facts concerning an individual or an event that are not available in any separate record.

Personal confidential data: This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this guide 'personal' includes the DPA definition of personal data, but 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 'sensitive' as defined in the Data Protection Act. Used interchangeably with 'confidential' in this document.

Personal data: Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy impact assessment: A systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure.

Processing: Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data.

Pseudonym: Individuals are distinguished in a data set by using a unique identifier, which does not reveal their 'real world' identity.

Public interest (test): This applies when the holder of the information believes that the public good that would be served by sharing the information outweighs both the obligation of confidentiality owed to the individual and the public good of protecting trust in a confidential service.

Re-identification: The process of analysing data or combining it with other data with the result that individuals become identifiable. Also known as 'de-anonymisation'.

Safeguarding: The process of protecting children and vulnerable adults from abuse or neglect, preventing impairment of their health and development, and ensuring they live in circumstances consistent with the provision of safe and effective care. It enables children to

have optimum life chances and enter adulthood successfully and adults to retain independence, wellbeing and choice and to access their human right to live a life that is free from abuse and neglect.

Sensitive personal data/information: Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual. See also 'Personal confidential data'.

Service user: An individual receiving social care services.