Data sharing guidance

Introduction

1. In 2013, Dame Fiona Caldicott's *Information Governance Review: information to share or not to share* introduced the seventh Caldicott principle: **The duty to share information can be as important as the duty to protect patient confidentiality.** This seventh principle was designed to encourage teams of professionals providing direct care for a patient or service user to share information across professional or organisational boundaries to maximise safety and quality of care.
2. All health and social care professionals have a responsibility to protect and maintain confidentiality, but they must also be aware of situations where other considerations (such as safeguarding) take precedence and override the duty of confidence, and must have the confidence to share information in the best interests of their patients and service users following the Caldicott principles.
3. This document has been produced as part of the Buckinghamshire-Oxfordshire-Berkshire (West) (BOB) Data Sharing Framework by the BOB IG steering group. Its purpose is to inform organisations, including GP practices, of the legal and statutory principles by which data may be lawfully and safely shared. It is hoped that the guidance will give data controllers the confidence to share data for patient benefit.
4. The guidance is based predominantly on the Caldicott principles (1997 & 2013) and covers the various legal bases for sharing – taking into account the General Data Protection Regulation (GDPR), which is being incorporated into the Data Protection Bill currently before Parliament — and the role of consent. In addition, those intending to share patient or service-user information should take into account relevant guidance from relevant organisations such as the Information Commissioner's Office (ICO), Information Governance Alliance (IGA) and professional regulators (see further guidance below).

Definitions

5. **Personal data**
   This generally means any data relating to an identified person–identifiable usually because it includes the person's name, though other items such as medical record number (MRN) or NHS number may enable the person holding the data to look up to whom it belongs.
6. The use of personal data is regulated by law. The Data Protection Act (1998) is the current relevant legislation. A new Data Protection Bill, which incorporates the provisions of the EU General Data Protection Regulation, is currently before Parliament and is expected to become law in early 2018.

7. **Personal confidential data, sensitive personal data, confidential patient information**
   These and similar categories refer to personal data that has been given in confidence or which contains items of a sensitive nature, meaning that particular care needs to be take when handling or sharing it and restrictions to its use may apply.
8. *Personal confidential data* was used throughout the Information Governance Review to mean personal information about identifiable individuals, which should be kept private or secret. '*Personal'* includes the Data Protection Act definition of personal data, but 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, adapted to include sensitive personal data as defined in the Data Protection Act.
9. *Confidential patient information* is defined in Section 251 (11) of the National Health Service Act (2006) and broadly includes personal confidential information relating to patients and users of social care services provided or arranged by local authorities.
10. *Sensitive personal data* as defined in the Data Protection Act includes characteristics such as ethnicity, politics, religious beliefs, trade union membership, physical and mental health, sexual life, offences. The GDPR definition includes in addition genetic and biometric data.
11. **De-identified data**
    Data from which items that could identify an individual have been removed. In its extreme form, data may be considered *anonymised*. The Information Commissioner's Office (ICO) describes anonymised data as "data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place."
12. A partial form of anonymisation, or *pseudonymisation,* allows individuals in a dataset to be distinguished from each other by means of a unique identifier which does not reveal their true identity.[1]
13. Although data protection law applies only to personal data, not anonymised data, note that the science of re-identification is now sufficiently advanced as to render the concept of anonymisation somewhat ineffective.[2]
14. **Data controller**
    An organisation or individual who determines the purposes for an manner in which personal confidential data are or will be processed. Data controllers must ensure that any processing of personal data for which they are

[1] It is common practice to maintain a separate table which combines the unique identifier and a real identifier. This is not strictly pseudonymisation, although if the table is kept securely separate from the de-identified dataset so that re-identification cannot take place, the latter is effectively anonymised.
[2] Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymisation. *UCLA Law Review 1701.*

responsible complies with relevant legislation. Data controllers are ultimately responsible for ensuring a legal basis for any data sharing.

15. **Direct patient 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, high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction, health or social care professionals and their team with whom the individual has a legitimate relationship for their care."[3]

16. **Information assets**
An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Key information assets, including all assets which include person-identifiable information, must each have a named information asset owner who is responsible for documenting and registering information assets and information transfers and ensuring their security.

The Caldicott principles

17. These principles are fundamental to the proper handling (processing) and sharing of personal data:

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.

[3] Department of Health (2013) *Information: to share or not to share. The Information Governance Review*

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.

Purpose

18. The first Caldicott principle – *Justify the purpose* — requires clarity about the reasons for sharing data. There are several situations where sharing patient data might be considered, e.g. for:

    - **Direct patient care** and its administration: the actual delivery of care by healthcare professionals and the necessary administrative and support functions to ensure safe and effective delivery and proper communication between those involved;
    - **Secondary uses** (see also below). These cover all uses of patient data other than for direct patient care, for example:
        - planning and commissioning of services;
        - monitoring and protecting public health;
        - compliance with statutory and legal obligations;
        - research.

19. The legal basis for sharing for each of these purposes may differ.

Lawful data sharing

20. The sixth Caldicott principle – *Comply with the law* – is often the most difficult to get right. Both data protection legislation and the common law duty of confidence need to be taken into account.

Direct patient care

21. Much of clinical care has traditionally been conducted on the basis of implied consent. However, consent is not necessarily the best basis for sharing data for direct patient care. Under the GDPR, "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including

by electronic means, or an oral statement." The GDPR therefore does not recognise implied consent.

Table 1: Possible legal bases for sharing patient data for direct care

	Legal basis		GDPR reference
Most relevant to health and social care			
1	Medical diagnosis and treatment		Article 9(2) (h)
2	The provision of health or social care		
3	The management of health or social care systems		
4	For the performance of a task carried out in the public interest or in the exercise of official authority		Article 6(1)(e)
Other possible legal bases for sharing			
5	Sharing is required by law	For example, the Children's Act 1989 requires information to be shared in safeguarding cases	Article 6(i)c
6	Overriding public interest	A formal public interest test should be undertaken	
7	Protection of vital interests	For example, to protect someone's physical integrity or life (either the patient's or someone else's)	Article 6(i)d
8	With the consent of the individual concerned	Provided the individual has mental capacity	

Secondary use

22. In general, the common law duty of confidentiality and implied consent will not provide a sufficient legal basis for secondary use. In some circumstances GDPR Articles 6(1)(e) or 9(2)(h) above may provide a basis, as may explicit consent [Article 6(1)a].
23. For many secondary uses, strict application of the 2nd and 3rd Caldicott principles (Page 3) will allow the use of de-identified data for the required purpose.
24. In circumstances where person-identifiable data is necessary for secondary purposes and it is genuinely impractical to obtain consent, for example for

retrospective research[4], then on the recommendation of the Confidentiality Advisory Group (CAG) of the Health Research Authority, the Secretary of State can set aside the common law duty of confidentiality to provide a legal basis (though not a mandate) to share. Applicants to CAG will need to convince the committee that obtaining consent is truly impractical.

Other relevant law includes:

25. **The Human Rights Act 1998** gives a right to respect for private and family life, which is relevant when confidential information about a patient or service user is shared. This right is not absolute, but any interference with a person's right to privacy must be necessary and proportionate. In general, this right will not be breached as long as sharing fulfils the obligations of the DPA and common law. In the event of challenge, the impact would be assessed by the court in relation to whether an ordinary person could have a reasonable expectation of privacy in the circumstances.
26. **Common law (or 'case law')** is law that has developed through courts making decisions in cases on legal points and creating binding precedents, in contrast to statutory law — which is determined by acts of parliament. It may be used to fill gaps in statutory provision, or to interpret what a statute might mean in particular circumstances.
27. **Duty of confidence.** There is no statutory provision which sets out a duty of confidence as such: the legal obligation is one of common law (the *common law duty of confidence*). This means that when someone shares personal information in confidence it must not be disclosed without some form of legal authority or justification. In practice, this will often mean that the information cannot be disclosed without that person's explicit consent unless there is another valid legal basis (Table 1, p.4). It is irrelevant whether the individual is old or has mental health issues or indeed lacks capacity.

Tools to facilitate safe and legal data sharing

28. **The BOB STP data sharing agreement and protocols framework**
To facilitate safe and legal sharing of patient information between organisations involved in the health and well-being of the population served by the BOB-STP, a sharing framework has been devised comprising the following:
    - An overarching data sharing agreement (DSA: Tier 1), signed by each participating organisation. This is effectively a memorandum of understanding that the signatory organisations will share patient information legally and safely; and
    - Separate data sharing protocols (DSPs: Tier 2) specifying for each discrete data flow its nature and purpose, the data set to be shared, the legal basis for sharing, security considerations and other relevant details.

[4] Although CAG comes under the Health Research Authority, is will consider applications for any secondary purpose, not just for research.

29. **Data protection impact assessment.** When establishing any new sharing data flow it is always good practice to consider privacy aspects ('privacy by design'), and this will become a legal requirement under the GDPR. A data protection impact assessment (DPIA) must therefore be undertaken at the outset. This will provide the necessary information to complete the sharing protocol.
30. For direct patient care a formal DSP may not be necessary provided that the DPIA is approved and agreed by both parties.
31. **Privacy (fair processing) notices.** The GDPR 'right to be informed' encompasses the obligation to provide fair processing information, typically through a privacy notice. It emphasises the need for transparency over how personal data is used. The ICO has produced guidance on the information which should be supplied in a privacy notice.

Further guidance

The Information Governance Alliance (IGA)

The Information Commissioner's Office (ICO)

General Data Protection Regulation (GDPR): FAQs for small public health sector bodies

The right to be informed/privacy notices

General Medical Council – Confidentiality guidance

A Manual for Caldicott Guardians

Authors

Maggie Lay, Clinical Transformation Lead,NHS South Central and West Commissioning Support Unit
Dr Chris Bunch, Caldicott Guardian Oxford University Hospitals NHS Foundation Trust

Version 1.0 2018-01-25