brownejacobson LLP

Confidentiality in a healthcare setting

This document is intended as a framework for informing decisions about sharing confidential information. It does not constitute legal advice. It arose out of a **Shared Insights** training session in January 2021, which was attended by professionals primarily from NHS Trusts. It has been prepared in that context on a free-of-charge basis.

Confidentiality in a healthcare setting

PART A: ALWAYS CONSIDER DISCLOSURE IN LIGHT OF THE DUTY OF CONFIDENCE

It has long been accepted that health information is confidential. This is due to the nature of that information and the way in which it is imparted to health professionals. The consequent 'duty of confidence' which arises over that information is the foundation of the relationship between health professionals and patients and, therefore, should inform all interactions involving requests to share patients' information. At its heart, this duty requires that those who are entrusted with confidential information keep it confidential, unless there is a lawful basis for overriding that duty. One key point to note is that the duty of confidentiality survives after death.

However, now that the duty of confidence is supplemented by a statutory framework governing personal information, it is only in relatively rare circumstances that the duty of confidence will need to be considered in isolation. Ordinarily, those handling health information will operate primarily under the specific statutory schemes which govern requests for access; information sharing arrangements; and disclosure more generally.

The key statutory schemes are:

- the data protection legislation (i.e. the UK GDPR[1] and the Data Protection Act 2018 ("DPA 2018")), which provides a 'right of access' for living individuals (or others acting on their behalf) to their personal data and, generally, governs the processing of living individuals' personal data; and
- the Access to Health Records Act 1990 ('AHRA') which enables a deceased patient's personal representative and any person who may have a claim arising out of the patient's death to apply for access to the patient's health records.

There are also other pieces of legislation that provide for information sharing in certain specific situations (such as is the case currently in relation to managing the Covid-19 pandemic) and there are other obligations arising in relation to disclosure, for example in a civil litigation context. In each of these scenarios, the duty of confidentiality underpins the statutory provisions.

The data protection legislation in particular is a comprehensive scheme which governs processing of personal data. This is supplemented by guidance published online by the Information Commissioner's Office which explains the Information Commissioner's expectations as to how the legislation will be applied in practice. In addition, the Caldicott Principles apply to the use of confidential information within health and social care organisations, as well as when such information is shared more widely.[2]

Although, broadly, if you comply with the data protection legislation, you will likely be meeting the obligations which arise out of the duty of confidence, the two legal frameworks aren't entirely overlapping and can involve a slightly different analysis to ensure they are being complied with. This is especially the case when you are considering a pro-active disclosure; dealing with a deceased individual's health and care information; or exploring new ways of working that might involve 'stretching' the duty of confidence to fit the modern health and care context[3]. All individuals working in a health and care context need to be aware of both aspects and understand when to seek advice.

[1] The UK General Data Protection Regulation as retained in UK law and read alongside the Data Protection Act 2018.
[2] The Principles were recently updated to include a new Principle 8: Inform patients and service users about how their confidential information is used. The principles will be supplemented by guidance on the appointment of Caldicott Guardian's in due course.
[3] Such as was the case in relation to the use of Google Deepmind's Streams application at the Royal Free NHS Foundation Trust.

Finally, we would also like to emphasise the seventh Caldicott Principle, which states as follows:

"The duty to share information for individual care is as important as the duty to protect patient confidentiality."

The key is to understand how and when to lawfully use confidential information.

When can the duty of confidence be overridden?

Health information can be disclosed without breaching the duty of confidence when any of the following circumstances applies:

The disclosure is in the "best interests" of a patient who lacks the capacity to consent

The patient consents, for the sake of their own care ("direct care") or for local clinical audit

The disclosure is required by legislation (e.g. in relation to deceased patients, under the Access to Health Records Act 1990 or a subject access request made under Article 15 of the GDPR) or a court order, or is for a permitted purpose, such as to a lawyer for the purposes of taking legal advice

The disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality (such as under section 251 of the National Health Services Act 2006)

There is an overriding public interest in disclosure, which weighs more greatly that the importance of preserving the patient's confidentiality

PART B: HANDLING OF REQUESTS

Check	Remember
Is the person entitled to make the request for this information?	The following can make a request for a patient's health data: • The patient, who is over 18. • A child patient as long as they are competent to do so.[4] • An authorised third party, provided proper written consent of a patient with capacity, lasting power of attorney or a court order has been provided. • An adult with parental responsibility where a competent child has authorised them to do so, unless it goes against the child's best interests. • An adult with parental responsibility for a non-competent child, provided the information hasn't been given in confidence and disclosure would not go against the child's best interests. Note that: • "Next of Kin" has no special legal status and care should be exercised when using this term. Some degree of authorisation (as above) is best but in practice, this will not always be possible and in that type of situation judgement will need to be exercised about whether someone with Next of Kin status has sufficient authority. • Requests by the Police are not subject access requests, but this type of data sharing will need to be lawful, necessary and proportionate as provided for in the data protection legislation, and you must ensure that disclosure would be compatible with the duty of confidentiality which arises over the information. We **recommend** developing separate internal guidance for staff dealing with such requests and working with your local police force to agree a framework to govern requests, where such requests are regular. • Divorce or separation does not affect parental responsibility unless there is a court order restricting such responsibilities or there are safeguarding concerns. • A personal representative, in respect of a deceased patient, and any person who may have a claim arising out of a patient's death, may request a "health records"[5] under the AHRA.
Is it a properly formulated request?	• A subject access request can be received in writing or verbally. Individuals can only be encouraged to use dedicated forms and processes. Where an individual makes a verbal request, a written record of the request should be made.

[4] *The Information Commissioner's view is that a child should not be considered to be competent if it is evident that he or she is acting against their own best interests. In a health and care context, a child's capacity should be considered in the context of how their care is being managed, consistent with the Gillick competence principles.*
[5] *Definition of Health Record in the AHRA context*

	• Where an application for a deceased individual's records are being made under the AHRA, the application should be made in writing. • You may need to verify the requestor's identity. If you are requesting ID documents, you should do so promptly. Where you have requested ID documents, the timescale for responding will not begin until you have received them. • It is okay to seek clarification or to ask for evidence of authorisation to act. See below.
When is the deadline to respond?	• The relevant statutory timeframes here are under the data protection legislation and the AHRA. You should respond to a subject access request *"without delay and at the latest within one calendar month."* So, if a request is received on 1 January it should be responded to without delay, with 1 February as the last day to respond. • Where an application under the AHRA concerns access to records or parts of records that were made in the 40-day period immediately preceding the date of the application, access to the records must be given within 21 days. Where the records have not been added to in the last 40 days, the request needs to be complied with within 40 days. • Consider also any internal KPIs you have for responding or any other deadlines set out in your organisation's policies. • For subject access requests made under the data protection legislation, you may extend the time to respond under by a further two months if the request is complex or you have received a number of requests from the individual, e.g. other types of requests relating to other of the individual's rights (such as the right to erasure).
Can we clarify the request?	• You may ask the requester to provide additional details about the information they want to receive and to clarify the scope of their request. When you do, the 'clock stops' until they respond.
Can we refuse the request entirely?	• Obligations arising out of the duty of confidence mean that such information can only be disclosed in the limited circumstances described on page 2 above. *"Access to confidential information should be on a need-to-know basis"*[6]. • Under the data protection legislation: if a subject access request is *"manifestly unfounded"* or *"manifestly excessive,"* you can refuse the request. 'Manifestly' means that there must be an obvious or clear quality to the unfoundedness or excessiveness. In other cases, the information should be disclosed unless an exemption applies as discussed in Part C below in which case the information may need to be withheld completely or, more likely, redacted. • Under the AHRA, access to a deceased person's records shall not be given where the record includes a note, made at the patient's request, that the patient did not wish for access to be given. There are also cases where access can be partially excluded, which are discussed in Part D below.

[6] *Caldicott Principle 4*

Have we conducted *"reasonable and proportionate"* searches?

Where conducting searches to comply with a subject access request, unless the individual has agreed to narrow the scope of the request, you need to search all the information the organisation holds. This includes (non-exhaustively):

- All electronic databases
- Blood test results
- Observation records
- Complaint files
- Handwritten records
- Serious Incident Reports
- GP Records
- Investigation results
- Post-operative records
- Lab results
- Letters
- Emails

PART C: CONSIDERING DISCLOSURE UNDER THE DATA PROTECTION LEGISLATION

Under the Data Protection Act 2018, there are a number of different exemptions from disclosure. Some apply to personal data generally. Some are specific to health data. Some are specific to other information which, in some contexts, the organisation is likely to hold (such as child abuse data or social work data).

It is beyond the scope of this checklist to set out and discuss the exemptions in full, but we would encourage you to ask the following questions about the information. If the answer to any of these questions is Yes, you should consider the relevant exemption in full and in such a situation, we also recommend you take advice from your medico-legal team, the organisation's Data Protection Officer or another legal or information governance professional.

Questions:

- Would disclosure of the individual's health data be likely to cause serious harm to the physical or mental health of any individual?
- Has the request about an individual been made by someone with parental responsibility for an individual under 18 (or someone appointed by the court to manage the affairs of an individual without capacity) and was the information provided by the individual in the expectation that it would not be shared?
- Would disclosure of the information involve disclosing information relating to another individual who can be identified from the information?[7]
- Was the information prepared for the purposes of litigation?
- Is the information communication between a lawyer and their client which came into existence for the purpose of giving or obtaining legal advice?
- Is the information that in respect of which a duty of confidentiality is owed by a professional legal adviser to their client?
- Is this a request for child abuse data being made by someone with parental responsibility for an individual under 18 (or someone appointed by the court to manage the affairs of an individual without capacity)?
- Does the information consist of information which was obtained from a local authority acting in connection with its social services functions, or from a government department, and would disclosure be likely to cause serious harm to the physical or mental health of the data subject or another individual?
- Is disclosure restricted by legislation (such as that which relates to human fertilisation and embryology information; adoption records and reports; statements of special educational needs; parental order records and reports; children's hearings)?

[7] *This will very often be the case. You can only disclose with the other individual's consent, or where it would be reasonable to disclose the information without such consent.*

PART D: CONSIDERING DISCLOSURE UNDER THE AHRA

As noted above, there are instances where access under the AHRA can be refused entirely. This is where the deceased person's record contains a note, made at the patient's request, that he or she did not wish for access to their records to be given.

Department of Health Guidance from 2010 qualifies this to say that such information can be disclosed if there is an overriding public interest, but that qualification is not made in the legislation itself. If you do consider there to be circumstances where the individual did not want their records to be disclosed after their death, but you suspect there may be an overriding public interest in disclosure, then we recommend you take legal advice and ensure your decision-making is appropriately documented.

Additionally, there are instances where the right of access to the deceased patient's records may be partially excluded. These operate as exemptions from disclosure and are similar to some of the main exemptions under the data protection legislation – albeit, the AHRA applies in relation to deceased individual's data.

The health and care organisation, as "holder" of the information, can partially deny access:

- Where in its opinion (having taken advice from an appropriate health professional) disclosure would cause serious harm to the physical or mental health of any other person.
- Where disclosure would identify a third person, who has not consented to the release of that information, unless the third person is a health professional who has been involved in the care of the patient.
- To records, or those parts of the records, which were made before 1 November 1991. This is unless, in the holder's opinion, having taken advice from an appropriate health professional, access would be necessary in order the make intelligible records which are disclosable.

Training proposal

Core training:

- Key legal principles and overview of the legal framework(s)
- Focus on confidentiality
- Case studies
- Q+A

£1,000 (plus VAT): 1-1.5 hour virtual session

Optional additions:

- The Data Protection Act 2018 in detail
- Managing complex information requests
- Information sharing with local partners (e.g. the police)
- Redaction – top tips
- Applying the exemptions under the Data Protection Act 2018
- Managing internal review/ICO involvement

extra £500 (plus VAT) to take the session to 1.5-2 hours duration

We can also include specialist training on:

- Data breach management
- Data claims management

Course option:

- Training on the topics mentioned above can also be delivered in modules across a number of dates at intervals of your choosing.

We are happy to work with you to adapt the training proposals above to suit your needs.

Please contact Charlotte Harpin, whose details are below.

Healthcare Information Law Team

Browne Jacobson LLP

Browne Jacobson's Healthcare Information Law Team provides information governance advice to the health sector. We have significant experience in advising and training NHS organisations on the legal frameworks relating to freedom of information, data protection and confidentiality. Our team of lawyers routinely advise on information governance policies and procedures, complex rights requests (including subject access), due diligence, information sharing, data breaches and reporting, access to health records, ICO investigations, claims and other litigation. We have been involved in a number of significant cases in the information law sphere.

Our lawyers are based across our offices and include junior lawyers and a paralegal with extensive experience assisting clients with redaction and complex subject access requests. We are also supported by a wider team of data protection and privacy lawyers.

We also advise on health tech issues, including supporting start-ups through our Grow programme, and support a number of ICSs as they implement information sharing arrangements to support partnership working.

We offer training sessions or modular courses on information governance matters. Please contact Gerard or Charlotte to discuss this further.

Gerard Hanratty
Partner and Head of Health

+44 (0)330 045 2159
gerard.hanratty@brownejacobson.com

Charlotte Harpin
Partner

+44 (0)330 045 2405
charlotte.harpin@brownejacobson.com

Dmitrije Sirovica
Senior Associate

+44 (0)115 976 6238
dmitrije.sirovica@brownejacobson.com

Matthew Alderton
Senior Associate

+44 (0)330 045 2747
matthew.alderton@brownejacobson.com

Steve Atkinson
Associate

+44 (0)20 7871 8515
steve.atkinson@brownejacobson.com

Contact us

Birmingham office

Victoria House
Victoria Square
Birmingham
B2 4BU

+44 (0)121 237 3900
+44 (0)121 236 1291

Exeter office

1st Floor
The Mount
72 Paris Street
Exeter
EX1 2JY

+44 (0)370 270 6000
+44 (0)1392 458801

London office

15th Floor
6 Bevis Marks
London
EC3A 7BA

+44 (0)20 7337 1000
+44 (0)20 7929 1724

Manchester office

14th Floor
No.1 Spinningfields
1 Hardman Square
Spinningfields
Manchester
M3 3EB

+44 (0)370 270 6000
+44 (0)161 375 0068

Nottingham office

Mowbray House
Castle Meadow Road
Nottingham
NG2 1BJ

+44 (0)115 976 6000
+44 (0)115 947 5246