The Common Law Duty of Confidentiality (CLoC)
a brief factsheet

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges (i.e. based on precedent).

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies (such as medical information provided by a patient to, or recorded by, a GP surgery, NHS Trust, local authority), that information **cannot** normally be disclosed without the patient's permission.

It is irrelevant for example how old the patient/client is, or what the state of his/her mental health is; the duty still applies.

Much like GDPR, the presumption is that *no such disclosure is permitted*, but that we must find an *exemption* to this rule if we are to allow it.

So, when we considering disclosing personal confidential information (i.e. health information) to a third party (an individual, the police, social services, a hospital, a data processor, the CCG/NHSE/NHSD/NHSX etc) we must **always** meet the CLoC in one of 4 ways:

1) The permission ("consent") of the patient. This can be:

    - Implied – e.g. when we send an eRS to a hospital consultant.
      The implied permission is that we will disclose only *necessary and relevant* information, in line with GDPR and GMC guidance.
      We can only rely on this for *direct medical care* purposes.

    - Express/Explicit – e.g. for most research disclosures, sending medical reports to insurance companies, certain audits, secondary uses.
      Normally, such permission is provided as "*written consent*", and/or clearly documented in the electronic GP record.

2) A Legal Obligation to disclose. Examples include:

    - NHS Digital (mandated by the HSCA 2012)
      Examples include the COVID-19 DPNs for at risk patients and pandemic research and planning
    - A court order
    - A direction from the SoS for Health under s3(4) of COPI 2002 for purely COVID-19 purposes (as in the UK Biobank disclosures that we were required to enable)

3) Overwhelming "public interest"

    This allows the disclosure of information for an individual, or individuals, where such disclosure is necessary to save their life or that of others.
    This is an exceptional way of meeting the CLoC, but is used in medical emergencies, in certain safeguarding situations (e.g. a s47 request as mandated by the Children Act 1989), and in some disclosures to the police.

4) Authority granted under The Health Service (Control of Patient Information) Regulations 2002 to set aside the explicit permission of the patient
This can be:

- Under Regulation 2 – Cancer
We rely on this to disclose for the purposes of the National Cancer Diagnosis Audit.

- Under Regulation 3(1) – public health emergencies
This is a tightly defined, and time-limited, regulation that *permits* (not compels) us to disclose *relevant and necessary* information, for *relevant* individuals, *purely* for such purposes (e.g. clearly COVID-19 related).
Providing a list of shielded patients to the community nurses could be justified under this (but other legal routes are more appropriate).

- Under Regulation 5, as authorised by the Health and Research Authority (so-called s251 CAG approval), for research and non-research purposes.
We rely on this to disclose to a data processor for the commissioned risk stratification for case finding services (CAG approval 7-04(a)/2013).

The burden is on us (the data controller) to always be able to demonstrate how we meet the CLoC, in one of those 4 ways, when any personal confidential information is disclosed from the GP surgery, for any particular purpose.
Each purpose requires a corresponding way of meeting the CLoC.

The CLoC is engaged whether we are disclosing personal confidential information about one patient or all of our patients.

Having GDPR legal bases for disclosure does not remove the need for permission or an appropriate legal basis (e.g. section 251 support) that meets confidentiality and ethical requirements. GDPR does not set aside either the CLoC or the Human Rights Acts.

What is **not** a legal basis in its own right to meet the duty of confidence?

- That an Article 6 and an Article 9 GDPR legal basis exists for such processing.
GDPR does not set aside the CLoC (or the Human Rights Act).

- That personal confidential information is being disclosed to a data processor (and subsequently to a sub-processor).
Organisations (such as Graphnet and Microsoft) do *not* have any legal right to access confidential personal information simply by virtue of being a data processor.

- That the data processor, or sub-processor, does not *routinely* access the information provided to it for processing.
Such an approach is a sound and necessary *security principle* - but it is not a legal basis in its own right to meet the duty of confidence.

- A belief, or assertion, that such secondary uses of information (primarily processed for direct medical care) is a "reasonable expectation" for an individual.
  "Reasonable expectations" does not meet the duty of confidence.

- That disclosed information is *pseudonymised at source.*
  Pseudonymisation is a security procedure, but neither renders personal data as non-personal, nor confidential information as non-confidential.

- That information is disclosed in an anonymised, or pseudonymised, format *at the end of the chain of processing.*
  The common law of confidentiality would only not apply if the information is completely anonymised *prior to disclosure by the data controller.*

- That *some* of the information disclosed has *a* processing purpose under Regulation 3(1), such as COVID-19.
  There must be a lawful basis under CLoC for the *entire* disclosure, linkage, onward disclosure, and *all* processing purposes.

- That an opt-out, or objection, to such processing exists for the individual.
  The right to object, or opt-out, is both a data subject right and enshrined in the NHS Constitution.

There cannot be unlawful "layering" of data protection; namely an assertion that – "downstream" – subsequent disclosures and processing might have a legal basis (e.g. CAG approval, COPI 3(1) processing, or that data is disclosed in an anonymised format), so purportedly rendering prior – "upstream" – disclosures and processing as lawful.

It is for us to ensure that the patient has actually given their explicit permission, or that a legal obligation actually does exists, or that there is a genuine emergency, or that disclosure absolutely complies with COPI 2002 and the very strict remit it provides.
The buck stops with us.

If any requested, or proposed, disclosure cannot meet the CLoC in one of those 4 ways then we cannot disclose – it would be unlawful and would result in a personal data breach (Art 33).

We should demonstrate how we meet CLoC for *all* our disclosures in our privacy notices.

We should demonstrate how we meet CLoC for *all* our disclosures in our DPIAs.

It should be the *first* thing that you think about when deciding whether to, how to, and who to, disclose health information (even before GDPR and considerations of purpose limitation, data minimisation, anonymisation etc).

The Common Law Duty of Confidentiality (CLoC)
a brief factsheet

GMC Guidance

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/using-and-disclosing-patient-information-for-secondary-purposes

80 You may disclose personal information without breaching duties of confidentiality when any of the following circumstances apply.

a. The disclosure is required by law, including by the courts (see paragraphs 87 - 94).
b. The patient has given explicit consent (see paragraph 95).
c. The disclosure is approved through a statutory process that sets aside the common law duty of confidentiality (see paragraphs 103 - 105).
d. The disclosure can, exceptionally, be justified in the public interest (see paragraphs 106 - 112).

85 If it is not practicable for the information to be anonymised within the direct care team, it may be anonymised by a data processor under contract, as long as there is a legal basis for any breach of confidentiality (see paragraph 80), the requirements of data protection law are met (see the legal annex) and appropriate controls are in place to protect the information (see paragraph 86).

Disclosures with specific statutory support

103 In England, Wales and Northern Ireland, statutory arrangements are in place for considering whether disclosing personal information without consent for health and social care purposes would benefit patients or the public sufficiently to outweigh patients' right to privacy. Examples of these purposes include medical research, and the management of health or social care services. There is no comparable statutory framework in Scotland.

104 Section 251 of the *National Health Service Act 2006* (which applies in England and Wales) and the *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016* allow the common law duty of confidentiality to be set aside for defined purposes where it is not possible to use anonymised information and where seeking consent is not practicable. You can find more detail about these statutory arrangements in the legal annex.

105 You may disclose personal information without consent if the disclosure is permitted or has been approved under regulations made under section 251 of the *National Health Service Act 2006* or under the *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016*. If you know that a patient has objected to information being disclosed for purposes other than direct care, you should not usually disclose the information unless it is required under the regulations.[40]

The Common Law Duty of Confidentiality (CLoC)
a brief factsheet

BMA Guidance

https://www.bma.org.uk/advice-and-support/ethics/confidentiality-and-health-records/disclosing-patient-data-for-secondary-purposes

Explicit patient consent is needed for the use of confidential patient information for secondary purposes.

Confidential patient information may be disclosed for secondary uses without explicit consent if:

- the disclosure of confidential patient information has been authorised by the Health Research Authority's Confidentiality Advisory Group (CAG) under section 251 of the NHS Act 2006 (in England and Wales)
- it is a disclosure made under the 'Confidentiality and Disclosure of Information Directions 2013'

  This provides a limited statutory basis for some specific disclosures where it is not possible to obtain express consent and where it is not feasible to anonymise data. These specific disclosures include secondary uses relating to the financial and management arrangements of the NHS, eg QOF reviews or investigating complaints
- it is otherwise required by law

NHS Digital Guidance

https://digital.nhs.uk/services/data-access-request-service-dars/dars-guidance/data-sharing-standard-7b---duty-of-confidentiality

When is disclosure of confidential information permitted?

There should be no use or disclosure of any confidential patient information for any purpose other than the direct clinical care of the patient to whom it relates, however there are some broad exceptions.

1. The patient explicitly consents to the use or disclosure.
2. The disclosure is required by law, or the disclosure is permitted under a statutory process that sets aside the duty of confidentiality.
3. The disclosure can be justified in the public interest.

The Common Law Duty of Confidentiality (CLoC)
a brief factsheet

COPI 2002 General Provisions (251 CAG "classes of support")

Circumstances in which confidential patient information may be processed for medical purposes under regulation 5 and particulars for registration under regulation 6.

1. The processing of confidential patient information for medical purposes with a view to making the patient in question less readily identifiable from that information.

2. The processing of confidential patient information that relates to the present or past geographical locations of patients (including where necessary information from which patients may be identified) which is required for medical research into the locations at which disease or other medical conditions may occur.

3. The processing of confidential patient information to enable the lawful holder of that information to identify and contact patients for the purpose of obtaining consent—

(a)to participate in medical research;

(b)to use the information for the purposes of medical research, or

(c)to allow the use of tissue or other samples for medical purposes.

4. The processing of confidential patient information for medical purposes from more than one source with a view to—

(a)linking information from more than one of those sources;

(b)validating the quality or completeness of—

(i)confidential patient information, or

(ii)data derived from such information;

(c)avoiding the impairment of the quality of data derived from confidential patient information by incorrect linkage or the unintentional inclusion of the same information more than once.

5. The audit, monitoring and analysing of the provision made by the health service for patient care and treatment.

6. The granting of access to confidential patient information for one or more of the above purposes.