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

Common law is not written out in one document like an Act of Parliament (*statute*). 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, or transferred and used, from that organisation - *"outside the data controller's own boundaries*" (to quote the ICO) - without the patient's permission.

Confidential information should only normally be shared when there would be "*no surprises*" for the individuals concerned: within the individual's *reasonable expectations.*

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

General Principles

Much like GDPR, the presumption is that *no such disclosure or use is permitted*, but that we must find an *exemption* to this rule if we are to allow it.
That is, **a way to avoid a breach of confidentiality** (a "*defence*" to any such allegation).

So, when we considering transferring 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:

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

  That is - it is **a reasonable expectation**, within health, that relevant and necessary information will be shared between health professionals who have a **legitimate, clinical, relationship** with the patient, for **direct medical care purposes**
  But - "*it's important to underline that the delivery of direct care is not of itself a catch-all to allow information to be shared under implied consent. The crucial thing is that information sharing must be in line with the reasonable expectations of the individual concerned." (NDG, "Reasonable expectations")*

  Confidential personal information can generally be shared on an implied consent basis for direct care when it is:

  - To inform and improve decisions about an *individual's* health and care

- By those who are *delivering care* to that individual or supporting such care, and
- It is reasonable to believe that the people concerned understand the information sharing involved, have indicated by their actions that they are content, and have not raised any objections

Express/Explicit – e.g. for most research disclosures, sending medical reports to insurance companies, certain audits, secondary uses, a s17 request from a local authority
Normally, such permission is provided as "*written consent*", and/or clearly documented in the electronic GP record
The patient must have both mental capacity and be able to give their permission freely and voluntarily
They should understand:

- who will see the information
- what is being disclosed
- the purpose of disclosure
- the significant foreseeable consequences

It is **not a reasonable expectation** that your personal, private, and confidential medical information will be disclosed/transferred/shared/given access to/used/processed, beyond your care team (e.g. your GP surgery) for any purpose beyond your direct medical care (secondary uses)

"Patients have a reasonable expectation that the information they share with their care teams will not be used for purposes beyond their own, individual care without their consent (save for certain permitted secondary uses to support the health and social care system). The duty of confidentiality requires that where confidential patient information is used for purposes other than an individual's own care and treatment, there must be either explicit consent, an exemption provided by law or an overriding public interest." (NDG 2022)

A Legal Obligation

to disclose (*disclosures required by statute*). Examples include:

- NHS Digital (mandated by the HSCA 2012)
- NHS Counter Fraud investigations (s.10 of the NHS Act 2006)
- Disclosures to the GMC – investigation of a doctor's fitness to practise
- Disclosures to the Health Service Ombudsman
- Coroner's investigations (Coroners and Justice Act 2009)
- A court order (both civil and criminal courts)
- The prevention and detection of certain crimes (e.g. terrorism, FGM)
- A notifiable infectious disease (Health Protection (Notification) Regulations 2010)
- A direction from the SoS for Health under s3(4) of COPI 2002 for purely COVID-19 purposes

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

Overwhelming "public interest"

(an example of a *permissive legal gateway*)

This *allows* (but does not compel) the disclosure of *necessary and relevant* information about an individual, or individuals, *where such disclosure is necessary* to save their life or that of others (sometimes referred to as "vital interests"), or otherwise felt warranted *in their best interest*.

It effectively applies the "*doctrine of necessity*".
This is an exceptional way of meeting the CLoC, but is used in medical emergencies, in certain safeguarding situations (e.g. s47 Children Act 1989), disclosures to MARAC *(if felt justified*; all victims referred to MARAC will have already been assessed as experiencing high risk domestic abuse by the agency who referred the case), in some disclosures to the police (if it is necessary for the prevention, detection, or prosecution of *serious* crime, in certain gunshot or knife incidents), disclosures to the DVLA , and where a patient lacks capacity.

It can also be justification to disclose certain genetic information, or information relating to a serious communicable disease:

"If a patient refuses to consent to information being disclosed that would benefit others, disclosure might still be justified in the public interest if failure to disclose the information leaves others at risk of death or serious harm (see paragraphs 63 - 70). If a patient refuses consent to disclosure, you will need to balance your duty to make the care of your patient your first concern against your duty to help protect the other person from serious harm." (GMC, Confidentiality)

Authority granted under The Health Service (Control of Patient Information) Regulations 2002

to set aside the explicit permission of the patient
(another example of a *permissive legal gateway*)
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)

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

Providing a list of shielded (CEV) 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), which is not regarded as *direct care* (hence the need for CAG approval)

The burden is on us (the data controller) to always be able to demonstrate how we meet the CLoC – *how we avoid a breach of confidentiality* - 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 our patients.

Having GDPR legal bases for processing (Article 6 and Article 9) does not remove the need for permission or an appropriate legal basis (e.g. section 251 support) that meets confidentiality and ethical requirements.
GDPR sets aside neither the CLoC nor the Human Rights Act.

Medical information is inherently:

- **Confidential**
- **Private**
- **Personal**

"It has always been accepted that information about a person's health and treatment for ill-health is both private and confidential. This stems not only from the confidentiality of the doctor-patient relationship but from the nature of the information itself."
Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457 at [145]

"As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some instances information may qualify for protection both on grounds of privacy and confidentiality."
Douglas & Ors v. Hello! Ltd & Ors [2007] UKHL 21 at [255]

That exposes data controllers (such as GP surgeries) to corresponding risks (heads of claim):

- A breach of confidence (common law, an equitable cause of action) ("BoC")
- A breach of privacy (a civil tort of misuse of private information) ("MPI")
- A breach of the Data Protection Act 2018 - unlawful processing under Article 5(1)(a) (a breach of statutory duty, right to compensation under Article 82 of UK GDPR)

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

Misuse of Confidential Information (MOCI, Breach of Confidence)

Legal precedent for breach of confidence stems from the 1969 case of *Coco v A N Clark (Engineers) Ltd: ChD 1968* at [419]. In that seminal case, Megarry J set out three elements ("tripartite test") which would normally be required if, apart from contract, a case of breach of confidence is to succeed:

1. **The information must be of a confidential nature**
   It must have the "necessary quality of confidence about it "
   Saltman Engineering Co Ltd v Campbell Engineering Co Ltd (1948) 65 RPC 203 at 215
   The circumstances in which the information is imparted will not be relevant where the information is obviously confidential (as explained in *Spycatcher* at [281-282])
   So, inadvertent access granted to confidential information does not diminish the confidential nature of the information.

2. **The information must have been communicated in circumstances importing an obligation of confidence**

   An obligation of confidence will, therefore, usually arise whenever someone receives information that they know - *or ought to know* - is confidential
   Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457 at [14]

   An *implicit obligation of confidence* arises between a patient and their doctor (sometimes referred to as an "*intrinsic nature of the relationship*").

   "There is no doubt that he relationship of doctor and patient carries with it a legal obligation of confidence in respect of confidentiality information concerning the patient gained by the doctor in his or her professional capacity"
   Toulson & Phipps on Confidentiality (4th Edn) at 5-004

   "the doctor is under a duty not to disclose, without the consent of his patient, information which he, the doctor, has gained in his professional capacity, save..... in very exceptional circumstances"
   Hunter v Mann (1974) QB 767 at [772]

   Information may be expressly or implicitly imparted in confidence.

   A duty of confidence will also be imposed where:

   - obviously confidential information is obtained by design, such as where an individual obtains the information improperly or surreptitiously
     Lord Ashburton v. Pape [1913] 2 Ch 469, or
   - deliberately and without authorisation takes steps to obtain the confidential information
     Inerman v. Tchenguiz [2010] EWCA Civ 908, [2011] 2 WLR 592, at [68]
   - by chance, such as where the document is dropped in a public place and picked up by a passer-by
     Attorney General v. Guardian Newspapers Ltd (No. 2) ("Spycatcher") [1990] 1 AC 109, at p281

3. There has been, or will be, an unauthorised use, or threat to use, dissemination, or disclosure of the information

The use of the confidential information will be unauthorised where no permission has been provided to the recipient to use or disclose the information, or if the information was disclosed for a particular purpose and has been used for another unauthorised purpose.

So,

- *used* for a purpose outside the bounds of what is permitted, and/or
- *disclosed or disseminated or transferred or communicated or supplied* to any other person, for a purpose outside the bounds of what is permitted, without authority or consent

Stadler v Currys Group Ltd [2022] EWHC 160 (QB) at [50]
PRACTICE DIRECTION 53B – MEDIA AND COMMUNICATIONS CLAIMS paragraph 8

An obligation of confidentiality can be breached by either:

- Disclosing confidential information to others
  OR
- Using the confidential information for an unauthorised purpose

"Disclosure" does not have to be made out, or proven, for a breach of confidence to occur. It is an example of misuse*, but not the only one*.
All there has to be is a *use* of information that is unauthorised and beyond the reasonable expectations of patients ("inconsistently with its confidential nature").

"Misuse will typically take the form of disclosure to another, but it need not do so."
Toulson & Phipps on Confidentiality (4th Edn) at 5-004

"Whether founded on contract or equity, the duty to preserve confidentiality is unqualified. It is a duty to keep the information confidential, not merely to take all reasonable steps to do so. Moreover, it is not merely a duty not to communicate the information to a third party. It is a duty not to misuse it, that is to say, without the consent of the former client to make any use of it or to cause any use to be made of it by others otherwise than for his benefit."
Bolkiah v. KPMG [1998] UKHL 52; [1999] 2 AC 222 at 235

To establish a breach of confidence, it is not necessary to establish that confidential information has been disclosed. It is sufficient that there has been misuse or a threat of misuse. The misuse occurs at the moment of *supplying the information to a third party*, for an unauthorised purpose, not at the moment when that information is read, or accessed, by the third party

"In our view, it would be a breach of confidence for a defendant, without the authority of the claimant, to examine, or to make, retain, ***or supply copies to a third party of****, a document whose contents are, and were (or ought to have been) appreciated by the defendant to be, confidential to the claimant*
(Tchenguiz v Imerman [2010] EWCA Civ 908; [2011] Fam. 116 at [69]).

The law of confidential information is not restricted to preventing unauthorised disclosures of confidential information. A person who has received information in confidence must not make unauthorised *use* of it.

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

An action for breach of confidence may be brought against a person who has used **or** disclosed, or threatened to use **or** disclose, confidential information without authority.

*"3.1 That there is an action for breach of confidence independent of statute has been beyond doubt for many years. Broadly speaking, it may be described as a civil remedy affording protection against **the disclosure or use** of information which is not publicly known and which has been entrusted to a person in circumstances imposing an obligation not to disclose or use that information without the authority of the person who has imparted it."*
The Law Commission report on Breach of Confidence 1981

*"The equitable doctrine of a breach of confidence seeks to protect confidential information from being **disclosed or used** for unauthorised purposes."*
ABC v Telegraph Media Group Ltd [2018] EWHC 2177 (QB) at [6]

*"most cases of breach of confidence involve either **use** of the information for the defendant's own purposes (for example, to develop a competing product or process to that of the claimant) or publication of the information (for example, in a newspaper). As can be seen from the excerpt quoted above, however, the Court of Appeal held in Imerman v Tchenguiz that it is a breach of confidence for a person merely to read a document which that person knows, or ought to appreciate, is confidential."*

*"It is well established that a person's unauthorised **use** of confidential information does not amount to a breach of confidence where that person has a lawful excuse for that **use**."*

*"If the third party knows or ought to appreciate that the information is confidential to the customer, then, as discussed above, the third party will come under an equitable obligation of confidence to the customer **not to use the information for any other purpose**."*

Primary Group (UK) Ltd & Ors v The Royal Bank of Scotland Plc & Anor [2014] EWHC 1082 (Ch) at [241] "Unauthorised use"

*"In a breach of confidence action, once it has been determined that an obligation of confidence exists, the claimant must next establish that the confidant has breached his obligation by making an unauthorized **use or disclosure** of the confidential information. Whether there has been a breach will be a question of fact involving a consideration of a number of issues. First it is necessary to examine how the obligation has been breached, **whether by use, disclosure, or some other act in relation to the information in question**."*
Tanya Aplin and others, Gurry on Breach of Confidence (2nd edn, OUP 2012) para 15.01

*"it is not necessary to show that a confidant has either deliberately or dishonestly misused information in order to establish that he has breached his duty of confidence. The duty is broken simply by an unauthorised **use or disclosure** of information"*
Tanya Aplin and others, Gurry on Breach of Confidence (2nd edn, OUP 2012) para 15.32

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

'It is not so much whether the defendant is careful with the information that matters. Rather what matters is whether information … has actually been misused'
Tanya Aplin and others, Gurry on Breach of Confidence (2nd edn, OUP 2012) para 15.41

"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."*
NHS Digital Section 2: The common law of confidentiality and consent

"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."*
NHS Digital: Data sharing standard 7b – Duty of Confidentiality

"When ***using*** *confidential patient information for purposes other than individual care, such as commissioning or research, you must always consider whether confidential patient information is actually needed. If confidential patient information is essential, then explicit consent is normally required for purposes beyond individual care. If it is not practicable to either work with anonymous data or to obtain explicit patient consent, then support under the Health Service (Control of Patient Information) Regulations 2002 is required. This is often known as 'section 251 support' (see section for IG professionals and HRA guidance for more detailed information)."*
NHS England: Consent and confidential patient information

"Common law requires there to be a lawful basis for ***the use or disclosure*** *of personal information that is held in confidence"*
UKCGC: The common law duty of confidentiality

"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"*
Confidentiality: NHS Code of Practice

"The classic case of breach of confidence involves the claimant's confidential information…..being ***used*** *inconsistently with its confidential nature by a defendant, who* ***received*** *it in circumstances where she had agreed, or ought to have appreciated, that it was confidential"*
Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] 1 WLR 1556 at [23]

It is perfectly feasible to lawfully *use* confidential information (e.g. for direct care, under "implied permission") without the recipient of the information *ever viewing or accessing it*.

It is also perfectly feasible to unlawfully use - *to misuse* - confidential information (e.g. for secondary purposes without s251 approval) without the recipient of the information *ever viewing it or accessing it*. That's what computers enable.

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

"Detriment", damage, or loss do not have to be made out or proven. Where the confidential information is private personal data, any use of that data which has not been authorised by the data subject is a misuse.

It is not necessary to show any detriment beyond the fact that the data is private and confidential and the use has not been authorised (Toulson & Phipps on Confidentiality (4th Edn) at [5-020 to 5-022]).

"if the defendants have deliberately and surreptitiously obtained, copied and stored the claimants' confidential information for the purposes of a competing business, in circumstances where the defendants knew or should have known the information to be confidential, that is sufficient to establish a breach of confidence as an equitable claim. It is not necessary to show that the defendants have specifically used the material in their business, or that the claimants have suffered loss and damage as a result."
Weiss Technik UK Ltd & Ors v Davies & Ors [2022] EWHC 2773 (Ch) at [123]

"If disclosure would be contrary to an individual's reasonable expectation of maintaining confidentiality in respect of his or her private information, then the absence of detriment … is not a necessary ingredient of the cause of action."
Bluck v ICO and Epsom & St Helier University NHS Trust (EA/2006/0090,17 September 2007) at [15]

The subject matter must be "**information**", and that information must be clear and identifiable.
Amway Corp v Eurway International Ltd (1974) RPC 82 at 86-87

The preservation of its confidentiality must be of **substantial concern** to the claimant (and not trivial or useless information).
Force India Formula One Team Limited [2012] ROC 29 at [223]

Where there has been inadvertent access granted to confidential information, a claimant does not need to show actual use or a threat to use. The fact that the recipient of the information, without the authority of the claimant or other legal authority, *refuses to delete it* upon request represents a breach of confidence. "Retention is enough".
Chief Constable of Kent Police & Anor v Taylor [2022] EWHC 737 (QB) at [54]

And, obviously, there must be **no defence** to the breach.

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

Misue of Private Information (MOPI, Breach of Privacy)

Article 8(1) of the Human Rights Act 1998 protects a person's right "to respect for his private and family life, his home and his correspondence".

"As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some cases information may qualify for protection both on grounds of privacy and confidentiality."
OBG Limited and others (Appellants) v. Allan and others (Respondents)Douglas and another and others (Appellants) v. Hello! Limited and others (Respondents)Mainstream Properties Limited (Appellants) v. Young and others and another (Respondents) at [255]

MPI is a distinct tort separate from Breach of Confidence.
Bloomberg LP v ZXC [2022] UKSC 5 at [45]

In respect to personal information, privacy is the right to have control over how your personal information is collected, disclosed, and used (data autonomy). And when you have been deprived of your right to control the use of your private information, then your right to privacy has been breached.

Individuals do not need to show financial loss (material damage) or distress to claim compensation. Damages can be awarded for "loss of control" – for the *fact of intrusion* (or the *commission of the wrong itself*).

> *"If one has lost "the right to control the dissemination of information about one's private life" then I fail to see why that, of itself, should not attract a degree of compensation, in an appropriate case. A right has been infringed, and loss of a kind recognised by the court as wrongful has been caused. It would seem to me to be contrary to principle not to recognise that as a potential route to damages."*
> Gulati & Ors v MGN Ltd (un-redacted) [2015] EWHC 1482 (Ch) at [111]

"Damages can and should be awarded for distress, damage to health, invasion of Sir Cliff's privacy (or depriving him of the right to control the use of his private information), and damage to his dignity, status and reputation."
Sir Cliff Richard v BBC and the Chief Constable of South Yorkshire Police [2018] EWHC 1837 (Ch) [350]

Information about an individual's private and personal life can be protected by the law of confidence, *even if disclosure would not result in any tangible loss to the confider*.
Any invasion of privacy resulting from a disclosure of private and personal information provided in confidence can be viewed as a form of *detriment in its own right*.

"a duty of confidence will arise whenever the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected."
Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457 at [14]

For a claim (tort of misuse of private information) to succeed it will be necessary to demonstrate:

1. The information was *private*

That is, the person to whom the information relates had a "reasonable expectation of privacy" in relation to the information ("Murray Stage One test")

"Essentially the touchstone of private life is whether in respect of the disclosed acts the person in question had a reasonable expectation of privacy"
Campbell v MGN Ltd [2004] UKHL 22 at [21]

and Ambrosiadou v Coward (Rev 1) [2011] EWCA Civ 409 (12 April 2011) at [30]

Our patients unquestionably have "*a reasonable expectation of privacy*". Where personal information is sensitive personal data for the purposes of the Data Protection Act 2018, such as medical information, that reasonable expectation of privacy is usually made out and the likelihood of distress being caused by its unlawful disclosure is increased

"*generally, details as to an individual's health are so obviously intimate and personal that a consideration of all the circumstances will result in that information being appropriately characterised as private under the stage one test unless there are strong countervailing circumstances*."
Bloomberg LP v ZXC [2022] UKSC 5 at [72]

2. That there has been an infringement of that person's *reasonable expectation of privacy*

Such as an *unconsented, or otherwise unauthorised*, disclosure, or transmission, or use of your personal, confidential, and private medical information (a *misuse* of your information)

3. And that expectation of privacy is not outweighed by a countervailing interest (such as the right to freedom of expression under article 10) – the "balancing exercise" ("Murray Stage Two Test")

- Ash & Anor v McKennitt & Ors [2006] EWCA Civ 1714 at [11]
- Murray v Big Pictures (UK) Ltd [2008] EWCA Civ 446 at (35]
- Stadler v Currys Group Ltd [2022] EWHC 160 (QB) at [49]
- PRACTICE DIRECTION 53B – MEDIA AND COMMUNICATIONS CLAIMS paragraph 8

There does *not* need to be proof of misuse.

"Mr White submits that proof of misuse is a separate and independent requirement of this tort. The argument did not go far on this issue, but I am not persuaded. I am content to deal with the case on the conventional two-stage test."
NT 1 & NT 2 v Google LLC [2018] EWHC 799 (QB)

Damages awarded in data protection have, to date, been smaller than those in other traditional reputation or privacy cases. For example:

TLT & Ors v The Secretary of State for the Home Department & Anor [2016] EWHC 2217 (QB)
Brown v Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724

A privacy claim may yield higher damages than a data protection claim. For example:

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

ZXC v Bloomberg LP [2020] EWCA Civ 611
Sicri v Associated Newspapers Ltd (Rev 1) [2020] EWHC 3541 (QB)
Richard v The British Broadcasting Corporation (BBC) & Anor [2018] EWHC 1837 (Ch)
Gulati v MGN Ltd [2015] EWCA Civ 1291

Breach of DPA/GDPR

Article 5(1)(a) of UK GDPR requires personal data to be processed *lawfully.*
This includes statute and common law obligations, whether criminal or civil.

Processing will be unlawful if it results in

- a breach of a duty of confidence, and/or
- a breach of the Human Rights Act 1998

Pursuant to *Article 82:* Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Or pursuant to s169 of the Data Protection Act 2018

Compensation for contravention of other data protection legislation

(1) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3).

(5) In this section, "damage" includes financial loss and damage not involving financial loss, such as distress.

In *Vidal-Hall v Google [2015] EWCA Civ 311* at [79], The Court of Appeal confirmed that claimants can claim for distress, *without having to prove financial loss*, for breach of the Data Protection Act 1998.

Lloyd v Google LLC [2021] UKSC 50

The Supreme Court has now confirmed that an award of *compensation* for a breach of the Data Protection Act 1998 ("DPA") can only be made where a data subject has suffered material damage, such as a tangible financial loss, personal injury, or psychological distress.

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

To recover compensation under section 13 of the DPA, it is not enough to prove a breach. In other words, an underlying breach (unlawful processing*) in and of itself* does not automatically entitle an individual to damages.

"Section 13 of the DPA 1998 cannot reasonably be interpreted as conferring on a data subject a right to compensation for any (non-trivial) contravention by a data controller of any of the requirements of the Act without the need to prove that the contravention has caused material damage or distress to the individual concerned".
at [138]

Not every data breach or unlawful processing of personal data is capable of giving rise to compensation (see the *de minimis threshold* section).

The Supreme Court's decision in Lloyd confirms that there are distinct differences between data protection and misuse of private information (MPI) as causes of action.

While accepting that 'loss of control' damages may be recoverable for misuse of private information (following Gulati v MGN Ltd [2017] QB 149), the Court held they are not recoverable for a breach of the Data Protection Act 1998.

"there is no reason on the face of it why the basis on which damages are awarded for an English domestic tort should be regarded as relevant to the proper interpretation of the term "damage" in a statutory provision intended to implement a European directive."
At [124]

The Supreme Court reiterated that MPI is a tort involving strict liability for deliberate acts. So, "loss of control" (or "loss of autonomy") damages *remain available* for breaches of the tort of misuse of private information - without proof of material damage or distress

Lloyd v Google and the DPA 2018/UK GDPR

The action giving rise to the claim in Lloyd v Google predates GDPR and was brought under the Data Protection Act 1998. While the relevant legislation is similar, it is remains to be seen whether a similar action brought in the future under GDPR may lead to a different outcome.

The Court was not considering the later legislation (i.e. the UK GDPR and DPA 2018), nor did it confirm how its findings apply in relation to the UK GDPR and DPA 2018 currently in force, and so this could potentially leave the door open for future loss of control claims under the GDPR.

The compensation regime under that legislation expressly refers to compensation being available in relation not only to material damages but also "non-material damages". Further, the recitals specifically reference *loss of control over personal data* as an example of possible damage resulting from a personal data breach.

So whilst the judgment has not ruled out the ability to bring a successful claim for damages on the basis of loss of control of personal data under the current data protection regime, it has definitely created a high threshold that must be established if such a claim were to succeed, as any claim under the current framework would need to differentiate itself from the precedent set by the Lloyd v Google UKSC judgment.

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

Positive wrongful action/Vicarious Liability

For a breach of confidence or breach of privacy claim to succeed, there must be *positive wrongful action by the data controller* – such as instructing a data processor to receive, use, process, and/or disclose information without authority (i.e. the data controller *purposefully facilitated it)* – as opposed to the actions of criminal third parties who have misused or disclosed the relevant data, no matter how egregious the controller's data security arrangements are; or for an employer who was in no way responsible for the criminal conduct of a rogue employee (acting "on a frolic of their own").

- WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12 (01 April 2020)
- Ali v Luton Borough Council [2022] EWHC 132 (QB)
- Darren Lee Warren v DSG Retail Limited [2021] EWHC 2168 (QB)
- Stadler v Currys Group Ltd [2022] EWHC 160 (QB)
- Smith & Ors v Talktalk Telecom Group Plc [2022] EWHC 1311 (QB)
- Cleary v Marston (Holdings) Ltd [2021] EWHC 3809 (QB)

BoC and MIP claims are primarily concerned with prohibiting activity *by the data controller* which is inconsistent with the concepts of confidence and privacy. Inadequate security measures (which nevertheless might constitute a breach of Article 5(f) of GDPR) do not involve the "use" of data.

De minimis threshold

Damages can be recovered for breaches of data protection regulations and misuse of private information, including for distress without specific pecuniary loss.

But for damages to be recoverable in a claim for a data breach or MPI:

- distress or damage over a *de minimis* threshold will need be proved, and
- that a person of "ordinary fortitude" would be distressed in that situation

There might be foreseeable factors which make claimants more vulnerable to distress, such as age, relevant pre-existing medical conditions, and other special circumstances

The de minimis principle developed through common law and confirms that whilst damages can, in principle, be recovered and other remedies obtained for breaches of data protection law and common law privacy torts, including simply for the distress caused, any distress must not be trivial in nature.

A remedy would not be granted where no harm has credibly been shown.

The complainant must have suffered actual damage; "*one cannot succeed in a claim where any possible loss or distress is not made out or is trivial.*"

When it comes to a breach, or misuse, of personal, confidential, private medical information, the de minimis threshold is likely to be met, as:

- Such information is *significant* (i.e. not low-level, or minimally significant, information)
- Such information is *especially personal and sensitive – special category data*

- Such information is not likely to involve "*a limited amount of personal data*"
- Such information is not likely to be to "*a single person*"
- There may well be clear evidence of "*onwards transmission*", or further dissemination, e.g. to a sub-processor
- There may well exist an "*ongoing threat to the individuals personal data*"
- The data controller may well be intending to continue such disclosure – to "*commission further torts*"
- Such a breach is *not likely to be trivial*
- In many cases, it will not be a "*one-off data breach that was quickly remedied*"
- In many cases, it is not going to be "*a mistake*" or due to "*human error*"
- It is unlikely to involve "*a third party briefly having access to anodyne personal information before promptly deleting it*"

Lloyd v Google LLP [2019] EWCA Civ 1599 at [55]

Rolfe & Others -v- Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB) : claims where the alleged distress or damage would not exceed a de minimis threshold should not proceed. Distress claims arising from fear of the unknown, feeling ill, and losing sleep worrying abut the possible consequences of a data breach fall below the de minimis threshold.

Claims are unlikely to succeed where:

- The breach poses a low risk of harm
- It only affects ordinary personal data, and not special category data
- It is promptly remedied , or prompt steps have been taken to mitigate the risks posed
- A person of "ordinary fortitude" would be distressed in such circumstances

Ashley v Amplifon Ltd [2021] EWHC 2921 (QB) : even where ancillary claims of BoC and MPI can continue in small data breach claims, the small claims track in the County Court can still be the appropriate forum.

Underwood v Bounty UK Ltd & Hampshire Hospitals NHSFT [2022] EWHC 888 (QB) : A data breach or MPI claim in which only the data subject's name, gender, and date of birth is compromised is unlikely to exceed the *de minimis* threshold for damages, meaning any such claim is unviable.

Johnson v Eastlight Community Homes Ltd [2021] EWHC 3069 (QB) : the de minimis concept and *Jameel* are equally applicable to claims under GDPR and DPA 2018, as it were to claims under the Data Protection Act 1998. The BoC and MPI claims did not add anything useful or independent to the claim arising for breach of the GDPR and are likely to obstruct the just disposal of proceedings. These claims were therefore struck out on the basis that they would take up disproportionate and unreasonable court time and costs.

Dow Jones & Co Inc v Jameel [2005] EWCA Civ 75 at [57]

A defamation case in which the Court of Appeal held that:

- the damage caused in that case was *minimal*, and
- the costs of obtaining it would be *disproportionate*, and
- to the detriment of the wider public in terms of *court resources*

- "*the game is not worth the candle*"

And so the claim was struck out. *Jameel* is therefore authority for the position that any such claim is an abuse of process and should therefore be struck out.

"After-the-event" Insurance

Claims for breaches of data protection law may be started in either the High Court (Media and Communications List, a specialist list of the Queen's Bench Division) or the County Court.

The County Court has no jurisdiction over BoC claims so this is yet another reason why claimants have persisted in issuing proceedings at the High Court.

Often, a claimant will make a claim for breach of data protection legislation, seeking damages at a relatively low value for the distress and anxiety they say has been caused by the breach.

But this claim will often be accompanied by parallel claims for one or more of:

- misuse of private information
- breach of confidence

Added on to the damages claimed will be

- the legal costs of the claimant's lawyers, together with
- the after-the-event ("ATE") insurance premium for the policy the claimant will have procured to bring a privacy claim

The BoC and MPI causes of action are one of the few remaining litigation claims where a claimant can recover his/her ATE premium from the defendant.

Claimants bringing data breach claims will typically have taken out ATE policies to protect them against any adverse costs and with a view to recovering an ATE premium if the claim is successful. They then seek to claim the premium on those policies back from the defendant. This will provide a substantial increase on the sums sought from the defendant, usually well in excess of the amount claimed.

Following the Jackson reforms, the recoverability of the costs of ATE insurance premiums from an opposing party in litigation was prohibited, but there is an exception to this for publication and privacy proceedings (i.e. where a claim is brought in privacy). Claimants are still entitled to recover ATE insurance premiums from defendants in those cases

This:

- *includes* claims for misuse of private information
- *includes* claims for breach of confidence

Claims for breach of data protection legislation are not "publication and privacy proceedings" under the Legal Aid, Sentencing and Punishment of Offenders Act 2012 ("LASPO").

As such, claimants are not entitled to recover ATE premiums from defendants in claims for breach of data protection legislation *alone*. This is one reason why BoC and MPI are often

"bundled" in with breach of GDPR/DPA claims (the other reason being the hope that the claim will proceed within the High Court and not be allocated to the "small-claims" track of the County Court - where parties are expected to bear their own costs, even if they pursue a successful claim).

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

What is not a defence against an allegation of a breach of confidence?

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

- "Implied consent" relied upon for the disclosure and use of (or *a* use of) confidential medical information for any purpose other than direct medical care

- That any disclosure, use, or processing, of confidential information automatically becomes a "reasonable expectation" simply by being described in a privacy notice
  A privacy notice is "fair processing information", a requirement under Article 13 of UK GDPR.
  But it is not a defence against a breach of confidence or privacy

- That personal confidential information is being disclosed to a data processor (and subsequently to a sub-processor), "accredited" or otherwise
  Organisations (such as data processors and sub-processors) do *not* have any legal right to receive, access, or use, private/confidential personal information simply by virtue of being a data processor

  Being "accredited" simply increases the confidence than any information will be processed securely by the recipient – Article 5(1)(f) of UK GDPR

- That a data processor is acting "under contract"
  Or an assertion that such processing is "controlled" within that contract

  A data processing/processor contract is a *legal obligation* under Article 28(3) of the UK GDPR
  Such a contract does not "lift" or "set aside" the CLoC.
  It does not "exempt" processing from the CLoC.
  It does not permit *uses* of the information beyond the reasonable expectations of patients (such as secondary uses).
  It does not provide the data controller with a defence against a breach of confidence or privacy.

- That a receiving organisation is being "transparent" about such processing

- That a receiving organisation has produced "a privacy notice" about such processing

- That a receiving organisation asserts GDPR legal bases to process the information *once received*

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

Neither a recipient's "privacy notice", nor its "transparency", nor how it "controls" the information it has received, nor how it claims it meets GDPR Article 6/9 legal bases, provide the data controller with a defence against an actionable breach of confidence and/or privacy.

- That the data controller discloses confidential information "within a system"
  Being a member of an ICB, or a PCN, or a GP federation, or a Shared Care Record (ShCR) scheme, does not provide a defence against a breach of confidence.
  It does not extend the data controller's boundary to include recipients of the information (including data processors) who might also happen to be a member of that ICB/PCN/Federation.

  Equally, a recipient of such information being a member of an ICB, or a PCN, or a GP federation, or a ShCR, does not authorise the use, or processing, of information beyond the reasonable expectations of the individual (such as for secondary uses of health data, including anonymisation, data analysis, and linkage).
- That there has been "consultation" about such processing
- That "similar processing" is already taking place for such purposes
- That the data processor, or sub-processor, does not *routinely* access the information provided to it for processing – and so "disclosure" has not occurred (so-called "automated" processing)

  It is absolutely the case that *every* data processor must not access the confidential information entrusted to it by the data controller without a lawful reason. The processor *may* have to access it (and *so must be able to*) in the investigation of data corruption, IT failure, when a data subject exerts their right to rectification or access, or when compelled to provide information to the ICO, the GMC, the PHSO, or the court.

  "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident"
  UK GDPR Article 32

  Such an approach is a sound and necessary *security principle*.
  It is a way for a data controller to demonstrate accountability, and their compliance with Article 5(1)(f).
  There must be information security and only justified access.
  It should/must be a *contractual* obligation on the data processor.

  "takes all measures required pursuant to Article 32"
  UK GDPR Article 28(3)(c)

  But such principles do not "lift" or "set aside" the CLoC.

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

The patient has still lost control of their confidential information.

A processor's dutiful compliance with Articles 28 and 32 does not "lift" or "set aside" the CLoC.

"It should be noted that an assurance (however binding) of maintaining confidentiality by someone receiving confidential patient information / personal data (who does not have a legitimate relationship with the person to whom the information relates), does not provide a legal basis for access/processing under the common law duty of confidentiality."
HRA: Types of health and care information and the legal frameworks protecting them

It does not "exempt" processing from the CLoC.
It does not permit *uses* of the information beyond the reasonable expectations of patients (such as secondary uses).
It does not provide the data controller with a defence against a breach of confidence or privacy.

It will still be a misuse, even if that information is unlikely to be accessed by staff at the data processor.

- 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 for purposes beyond direct medical care

  "Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways."
  Confidentiality: NHS Code of Practice

- That the use of the confidential information has "public benefit"
  Public benefit (as distinct from public interest) is subjective, and processing that is asserted to be in the public benefit (by one individual or organisation) does not set aside the common law of coinfidentiality.

- That disclosed information is *pseudonymised at source*
  Pseudonymisation is a security procedure – *a safeguard* (like encryption) - consistent with Article 32(1)(a) and Article 5(1)(f) of UK GDPR

  Pseudonymisation reduces the risk to individuals but, unlike anonymisation, does not take data out of the scope of data protection law.

Pseudonymisation neither:

- renders personal data as non-personal, nor
- renders personal confidential information as personal but non-confidential, nor
- renders private information as non-private (i.e. "public")
- changes the *nature* of the information (i.e. confidential/private/personal health data about an individual), nor
- changes *how* that information was obtained or generated (i.e. by a person who, in the circumstances, owed an obligation of confidence to that individual), nor
- changes *why* the information was obtained (i.e. recorded in the medical record) - the *purpose* for the original processing (direct medical care), nor
- diminishes, or removes, a reasonable expectation of how one's personal information would be disseminated and/or used, nor
- diminishes, or removes, a reasonable expectation of confidentiality or privacy

"However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the UK GDPR."
ICO, What is personal data?

"Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
Recital 26 GDPR

"Data that is capable of identifying individuals is subject to both the data protection law and the common law duty of confidentiality."
NDG: The right to privacy; digital data (2022)

"Where confidential patient information has undergone pseudonymisation, but the identity of the individual is ascertainable indirectly from information in the possession of, or likely to come into the possession of, the person processing that information, it remains confidential patient information. You will therefore require a legal basis to lift the common law duty of confidentiality before it can be disclosed to a potential recipient."
HRA : Confidential patient information that has undergone pseudonymisation

- 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 were completely anonymised *prior to transfer by the data controller*

  Anonymisation is itself a 'use' of identifying information under the DPA.
  And it is a *secondary use* - by definition, it *cannot be used for direct medical care.*
  It counts as processing for the purposes of data protection law.
  R v Department of Health, ex parte Source Informatics Ltd - [2000] 1 All ER 786

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

"*If we anonymise personal data, does this count as processing?*
Yes. For the purposes of data protection law, applying anonymisation techniques to turn personal data into anonymous information counts as processing" (ICO)

"You should also note that when you do anonymise personal data, you are still processing the data at that point."
ICO: What is personal data?

*"While confidential patient information that is rendered anonymous is no longer confidential patient information**, the process of accessing confidential patient information in order to render it anonymous is subject to the duty of confidentiality**."*

*"Where the anonymisation is to be performed by anyone else who does not have a legitimate relationship, there will be a disclosure of confidential patient information, albeit solely for the purposes of anonymising it**, and a legal basis to lift the common law duty of confidentiality is required.**"*
HRA: Types of health and care information and the legal frameworks protecting them

Patients have not given implied permission to doctors passing on their personal data to data processors, to be anonymised or pseudonymised, before being used for secondary medical purposes. That is not *direct medical care.*

*"A member of a patient's or service user's **care team** may render confidential patient information anonymous without breaching the duty of confidentiality. The care team includes registered health and social care professionals and other staff that directly provide or support care to patients"*
HRA: Types of health and care information and the legal frameworks protecting them

"Who can anonymise information?

It is not a breach of confidentiality if information undergoes anonymisation or pseudonymisation processes within the direct care team for a purpose that would be within patients' reasonable expectations (see section 3).
*A lawful justification (see section 1) is required **if confidential information is to be disclosed to a third party outside of the direct care team** in order to undergo anonymisation or pseudonymisation processes."*
BMA : Confidentiality toolkit

A data processor is *not* a member of the patient's care team.

*"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**".*
GMC : Using and disclosing patient information for secondary purposes at [85]

such as Regulation 5 COPI 2002 Class 1 authorisation (or "support"):
"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"

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

- That information is *encrypted in transit*
  Encryption is a security procedure – *a safeguard* (like pseudonymisation) - consistent with Article 32(1)(a) and Article 5(1)(f) of UK GDPR
  Encryption reduces the risk to individuals but does not take data out of the scope of data protection law

- 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 *ultimately* 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. That is called accountability.

If any requested, or proposed, disclosure cannot meet the CLoC in one of those 4 ways then we cannot disclose – it would be unlawful.
The duty of confidentiality is a legal right to prevent transmission of such information to another person in breach of a confidential (doctor-patient) relationship.

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.

The *first* legal basis: lawfulness under the **law of confidentiality** - *Seek advice from your **CG***
then
The *second* legal basis: lawfulness under **data protection** - *Seek advice from your **DPO***

"Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community."
Z v Finland (1997) 25 EHRR 371, 405, at [95]

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

"If people feel that their information may be used in unexpected ways, for purposes they may not support, this greatly undermines the fundamental relationship of trust. The effect may be to deter patients from seeking treatment, or, when seeking treatment, to only disclose partial or false details, thereby denying clinicians the information they need to deliver safe and effective care." (NDG, 2021)

"Patients using health and social care services are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters with healthcare professionals without fear that the information may be improperly disclosed. These services cannot work effectively without the trust that depends on confidentiality."
NDG written evidence submission to STC inquiry 2022: The right to privacy: digital data

---

"I will respect the secrets that are confided in me, even after the patient has died"
Declaration of Geneva, 2017

Confidential patient information

is defined in section 251 of the NHS Act 2006:

11. For the purposes of this section, patient information is "confidential patient information" where:

- *a. the identity of the individual in question is ascertainable*
  - *i. from that information, or*
  - *ii. from that information, and other information, which is in the possession of, or is likely to come into the possession of, the person processing that information, and*
- *b. that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual*

"Confidentiality, once breached, is lost for ever"
Cream Holdings Limited and others (Respondents) v. Banerjee and others (Appellants) [2004] UK House of Lords

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/media/4283/bma-confidentiality-and-health-records-toolkit-july-2021.pdf

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, e.g. QOF reviews or investigating complaints
- it is otherwise required by law

It is not a breach of confidentiality if information undergoes anonymisation or pseudonymisation processes within the direct care team for a purpose that would be within patients' reasonable expectations.

A lawful justification (see section 1) is required if confidential information is to be disclosed to a third party outside of the direct care team in order to undergo anonymisation or pseudonymisation processes.

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

NHS England Guidance

https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/

When using confidential patient information for purposes other than individual care, such as commissioning or research, you must always consider whether confidential patient information is actually needed.

If confidential patient information is essential, then explicit consent is normally required for purposes beyond individual care. If it is not practicable to either work with anonymous data or to obtain explicit patient consent, then support under the Health Service (Control of Patient Information) Regulations 2002 is required. This is often known as 'section 251 support'

Other Guidance

- Information Sharing in Cases of Domestic Violence and Abuse (UKCGC)
- Information sharing and suicide prevention: consensus statement (DHSC)
- Police information requests to NHS Organisations, GPs and other healthcare providers in respect of potential homicide investigation, proof of life enquiries and more general enquiries to trace missing persons (NCA/UKCGC)
- IG Framework for Integrated Health and Care: Shared Care Records (NHSX)
- NHSX letter to DPOs regarding the transfer and use of confidential medical information to ShCR data processors for purposes other than direct care
- Manual for Caldicott Guardians (UKCGC)
- Confidentiality - guidance for registrants (HCPC)
- The Common Law Duty of Confidentiality (HEALTH-NI)
- Medical disclosure information to attorneys and deputies (OPG)
- GDPR: Lawful basis, research consent and confidentiality (UKRI/MRC)
- Disclosure to third parties (MDU)

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

- An introduction to confidentiality (MDU)

Letter from NDG to NHX December 2020 regarding Shared Care Records
https://www.nhsdatasharing.info/NDG2NHSX.pdf

First letter from NHX to Shared Care Record Schemes May 2021
https://www.nhsdatasharing.info/NDG%20Data%20Enquiry.pdf

Second letter from NHSX to Shared Care Records Schemes Sept 2021
https://www.nhsdatasharing.info/NHSXLetter.pdf

Letter from NDG to ICBs regarding Shared Care Records
https://www.gov.uk/government/publications/letter-to-integrated-care-board-siros-from-the-national-data-guardian-and-uk-caldicott-guardian-council/letter-to-icbs-from-ndg-and-ukcgc-issued-7-november-2022

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.

Class 1 support – extraction and anonymisation/pseudonymisation of the 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.

Class 2 support – geographical location (research)

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.

Class 3 support – seeking consent (research)

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.

Class 4 support – linkage of information from more than one source

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

Class 5 support – auditing, monitoring, and analysis of direct patient care

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

Class 6 support