GDPR: Lawful basis, research consent and confidentiality

This guidance is for Data Protection Officers (DPOs) in research organisations, research and governance managers (NHS, university, MRC or other), researchers (who collect and use personal data to support their research), and those who supply data to others for research (e.g. GP, hospital and central NHS data). It has been developed with the participation of the Information Commissioner's Office (ICO) and others.

This guidance will cover the following:

- the most likely lawful basis to hold and use (process) personal data[1], and special category personal data[2] to support research;
- why consent is important in research (it is unlikely to be your lawful basis);
- the difference between data protection and the common law of confidentiality (the requirement to respect the duty of confidence will not change); and
- how the national patient opt-out programme (National Data Opt-out) in England relates to the common law of confidentiality.

The spirit of GDPR is to ensure organisations are **lawful**, **fair** and **transparent** when holding and using personal data. Scientific research has a natural route through the law which depends on specific safeguards being in place. You will have most of these safeguards in place already, in the processes and procedures that form accepted good practice for scientific research using personal data. For example:

- Research Ethics Committee approval,
- Governance checks (including HRA assessment),
- Peer review from public funders,
- Data minimisation and minimisation of recruitment numbers,
- Pseudonymisation and other technical safeguards against accidental disclosure and loss or corruption of research data, etc.

Such safeguards are necessary to assure data subjects (research participants) that your organisation takes its legal and ethical responsibilities towards them, and their data, seriously.

---

[1] Personal data: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[2] Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health or data concerning sex life or sexual orientation.

1. Lawful Basis

Data protection law allows organisations to hold and use (process) personal data if they have a legal reason to do so (i.e. if they have a lawful basis). The law demands that organisations specify the lawful basis they are using to process personal data and are explicit about this. In other words, DPOs need to identify the acceptable reasons (defined in law) to process personal data and make research participants aware of this. These legally acceptable reasons are defined in GDPR and listed in the Appendix. Organisations must specify one of the reasons given in Article 6 to process personal data and an additional reason provided in Article 9 to process special category personal data (see footnote on page 1 for definitions).

The intention of the law is to allow organisations that need personal data to support their legitimate activities, to do so. The lawful bases available depend on whether your organisation is a public authority or not.

Public authorities (e.g. universities, NHS, research council institutes) are funded by the public purse in order to conduct tasks that are in the public interest. Therefore, the legal reason that public authorities will have to process personal data is most likely to be:

Article 6(1)
*(e) processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested the controller;*

The Explanatory Note to the Data Protection Bill clearly states that research in universities should be able to rely on this lawful basis ('public task'). As does the ICO. DPO's need to evidence this by reference to their public research purpose as established by a university's constitution (e.g. University Charter) and legal powers; or relevant statute (e.g. Higher Education and Research Act, 2017).

For research conducted by other organisations, such as charity research institutes that are not public authorities, and commercial companies, the most appropriate lawful basis is likely to be:

Article 6(1)
*(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

By using either 'public task' or 'legitimate interests' you assure research participants that your organisation has a genuine reason to process personal data. This is in addition to the control you give participants through the normal consent (to participate in research) process.

2. Special category personal data

Most health research uses **special category** personal data. These are defined as:

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health or data concerning sex life or sexual orientation.

Research organisations that hold and use (process) special category personal data must ensure that they have a lawful basis to process personal data (section 1 above, GDPR Article 6), and an additional condition to process special category personal data (GDPR Article 9). You can find a list of all available lawful bases and conditions in the Appendix.

The law was written with research in mind, in fact one of the additional conditions for holding and using special category personal data (for all organisations, public authority or otherwise) is:

Article 9(2)(j)
processing is necessary for archiving purposes in the public interest, scientific or historical ***research purposes*** *or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

This refers to Article 89(1) which outlines safeguards that are likely to be present in most scientific research already (see safeguards on page 1). Research is managed tightly within universities, research council institutes, NHS, charities, etc. through governance mechanisms. These governance arrangements provide research participants with assurance that their personal data is:

- **Necessary** to support research,
- Will only be used to support **legitimate** research activities considered to be in the **public interest,** and
- Their interests are **safeguarded**/**protected.**

These organisational assurances are in addition to the controls research participants have on the use of their personal data through the normal research consent process.

DPOs need to ensure that the policies and procedures in place in their organisations are appropriate to manage the risks posed to all data subjects (including research participants). For more information on the safeguard requirements see HRA technical guidance.

3. Consent and data protection law

We have not discussed consent in much detail in this guidance. Informed, voluntary and fair consent is the cornerstone of ethical research involving people. It is a mechanism, to ensure the rights of individual participants can be respected. It is through the consent process that research participants can understand what taking part in a specific study will mean for them, so they can make an informed choice and feel able to express their wishes.

Yet consent is not likely to be your **lawful basis** to hold and use (process) personal data, or the condition to process special category personal data, for research. The Information Commissioner's Office (ICO) has published a blog article: Consent is not the 'silver bullet' for GDPR compliance.

Data protection law requires organisations to be **fair and transparent** in how they process personal data. In other words, organisations must be open and honest with research participants about how they intend to use personal data, and the types of data they will be using, etc. The consent process, whilst not being the only way, aids transparency and fairness for research participants.

The ICO recommends a layered approach to transparency. Project-specific information (the information you provide to participants during the consent process) should not be the only information made available to research participants. In addition, organisations may provide corporate level and possibly departmental level / research group level information. All these sources should align and complement each other. Therefore researchers, research governance leads, Clinical Trials Units and DPOs should work together to ensure a joined-up approach to transparency.

Transparency information must be concise, clear and easy to understand. Consider the audience; use clear, plain language; and ensure transparency information is easily accessible. For more information see the ICO web pages, HRA technical guidance and Article 29 Working Party Guidelines on Transparency.

Other parts of the law do demand that consent is in place before research can happen (e.g. Human Tissue Act, Medicines for Human Use (Clinical Trials) Regulations, etc.). Later in this guidance we will consider when consent is required by the common law to **manage confidentiality**. Given the additional ethical imperative to obtain consent whenever possible, researchers should review and improve their consent procedures in line with good research practice. (See HRA/MRC Consent and participant information sheet preparation guidance).

The law does provide the lawful basis of 'consent' to process personal data; and 'explicit consent' as a condition for special category personal data. However, we envisage that research organisations will not need to rely on these to support their research activities where an alternative lawful basis such as those suggested above can be identified. The types of organisation that may need to rely on consent are those involved, for example, in marketing, who have traditionally used pre-ticked boxes to indicate agreement to share personal data widely.

4. Common law - confidentiality

The law around information about people is further complicated in the UK as we must also comply with the common law of confidentiality. Common law is no less important than statute (i.e. law that is written down in Acts, Regulations, etc. and passed by Parliament). You should be aware that **the requirement to respect any duty of confidence when accessing or sharing confidential information for health research, will not change.**

Information is considered confidential in law if:

- It can be related to an identifiable individual (*similar definition of identifiable as used for personal data, but personal data can only relate to a living person, confidential information can relate to the living or deceased)*, and
- It is not in the public domain *(no such limit is placed on the definition of personal data)*, and
- It is given with the expectation that it will be kept confidential. Individuals do not have to be explicit about their expectations, when entrusting others with their information: this expectation is often implicit, given the relationship the individual has with their doctor, nurse, researcher, etc.

When an individual entrusts a research team, or a clinical care team, with confidential information, the team must handle this in line with '**reasonable expectations'**. In other words, confidential information should only normally be shared when there would be '**no surprises'** for the individuals concerned.

Precisely what a reasonable person might expect can be difficult to define. We can assume that reasonable patients do expect their confidential information to be shared within their clinical care team. In some cases, the clinical care team may include researchers. In such circumstances, patients would not be surprised if all their care team, including researchers, were party to their confidential information. However, not all researchers will have this relationship with patients[3].

We know that not many people understand collaboration is common in research or how confidential information may be shared as part of collaboration. Where participants would not expect you to be sharing their confidential information with others, you can manage their expectations by informing them of your intentions (e.g. in project materials or during discussions about participation) and asking them if they are happy with these plans. There is no need to inform participants of every complex technical detail of how their confidentiality will be respected. They should understand what is being proposed and what this might mean for them, before they decide whether you can share their confidential information with others.

You should always consider if you could limit the sharing of information to robustly anonymised information only. Robustly anonymised[4] information can be shared without having to consider reasonable expectations (Information has to be **identifiable** to be subject to the common law of confidentiality).

There are specific times when organisations may wish to share confidential information, for example to prevent a crime from being committed and/or where there are safeguarding concerns. In such cases, disclosing the information rather than keeping it confidential, best serves the public interest. The common law does allow disclosure when it is in the overwhelming public interest, even if the person involved might not expect this.

---

[3] Sections 3.6 and 3.7 of Information to share or not to share: The Information Governance Review.
[4] ICO Anonymisation Code for further guidance.

5. Disclosure to support research – outside reasonable expectations

In the UK there are legal avenues that allow the disclosure of confidential information to support medical research, even when this is not in line with 'reasonable expectations' (i.e. without consent).

In England and Wales, such disclosure can be approved ('section 251 approval') by the HRA who are advised by the Confidentiality Advisory Group (CAG); in Scotland approval can be sought from the Public Benefit and Privacy Panel for Health & Social Care (PBPP); and in N. Ireland advice can be sought from the Honest Broker Service (HBS).

Approvals to disclose confidential information outside reasonable expectations do not affect an organisation's legal obligations to abide by data protection law for the personal data they hold. In research scenarios where section 251 approval (or another legal avenue for disclosure) is in place, and the confidential information being disclosed would also be classified as personal data, the organisations holding this data (both the organisation disclosing the information and the recipient organisation) must also:

1. have a lawful basis to process personal data, and
2. if applicable, have a condition to process special category personal data, and
3. be **fair** and **transparent** about how they hold and use (process) this data (see fair and transparent on page 4). Be aware that when HRA CAG approves disclosure, they require researchers to provide additional notification to the relevant patient population, so called 'patient notification'.

6. National patient opt-out programme and the common law

The national patient opt-out programme in England (National Data Opt-out) provides patients with an opportunity to opt out of specific non-care related uses of confidential patient information (anonymised information is not subject to opt-out). Patients can opt-out and have their preference applied widely across the health and social care system. (This replaced the Type 2 opt-outs which only applied to confidential patient information flowing from NHS Digital).

The national opt-out applies to the disclosure of confidential patient information under the common law, and not through data protection. It must not be confused with the right to object under the data protection law. As such, opt-outs do not apply where consent for disclosure for a research project is in place. As we have seen in Section 4, consent allows disclosure of confidential patient information to others for other purposes, as long as this disclosure is in line with reasonable expectations, i.e. there are no surprises.

Section 251 approval from CAG requires opt-outs to be respected as patients have expressed a wish that their confidential patient information not be disclosed for non-care purposes, and because consent for disclosure is not in place. *However, CAG can, in exceptional circumstances, approve an application that has robust justification for opt-outs to be overridden, for example 100% inclusion is statistically required. In such rare situations CAG can deem that there is an overriding public interest for the research to go ahead without opt-outs being upheld.*

It is worth noting that irrespective of a patient's opt-out status, Dame Fiona Caldicott has been very clear that all patients have a right to be invited to take part in research. (See National Data Guardian review: *'People should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care'.)*

7. Putting it all together

Consent to participate in research is at the heart of ethical research. Discussions about participation, and the information provided during the consent process, can help ensure that data is transparently held and used for research. Consent can help organisations act **fairly and transparently**, as required by data protection law. Consent can help **manage expectations** in terms of who has access to confidential information (common law). Additionally, consent may be required for other legal reasons (e.g. Human Tissue Act, Medicines for Human Use (Clinical Trials) Regulations, etc.). Research organisations should ensure that consent is obtained from research participants whenever possible. Consent is only meaningful if participants **understand** what is being asked of them. They must be able to consider any **significant risks** to their safety, their rights and their dignity. They must be able to make a **voluntary** decision, free from undue influence and they must be **competent** to make such a decision.

Data protection law does not demand consent (explicit or otherwise) to be in place to hold and use (process) personal data (including special category personal data). Organisations must have a **lawful basis** to process personal data, they must be **transparent** and ensure that individuals are treated **fairly**. In the UK, the most likely lawful basis for public authority research organisations to process personal data for research is **public task -** Article 6(1)(e). For non-public authorities it is likely to be **legitimate interests** - Article 6(1)(f). In addition, organisations (public authority or otherwise) that process special category personal data for scientific research should be able to demonstrate that **processing is necessary for scientific research purposes in accordance with safeguards** - Article 9(2)(j). Once organisations have identified their most appropriate lawful basis and condition, they must document these and comply with the rest of the law (please also see the ICO web pages and the HRA technical guidance).

Common law dictates with whom confidential information can be shared. The common law demands that confidential information is managed in line with **reasonable expectations (no surprises)**. Expectations can be managed by consent (implicit or explicit). The common law does allow disclosure even when this might not be reasonably expected, if disclosure is in the **public interest**, or **another legal avenue** is established (e.g. with section 251 approval).

The **national patient opt-out** enables patients to opt out of their confidential patient information being disclosed outside the duty of confidence; unless consent (in line with reasonable expectations) for disclosure for a research project is in place. Opt-outs can be overridden in exceptional circumstances by HRA CAG. Anonymised flows of information are unaffected by opt-outs. All patients, irrespective of their opt-out status, have a right to be invited to take part in research.

Appendix

GDPR

Article 6 Lawfulness of processing - [Lawful bases]

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

GDPR

Article 9 Processing of special categories of personal data - [Conditions]

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the

provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.