Preparation for the implementation of the General Data Protection Regulation (GDPR): Understanding the current legal situation

Guidance note 2

This guidance is for Data Protection Officers (DPOs) of research active 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 (to support research conducted by others).

Developed in consultation with the ICO and others, this is the second in a series of guidance notes preparing for GDPR. The first guidance note focused on knowing what personal data you hold.

When GDPR is implemented, DPOs will need to know which legal basis their organisation has to hold personal data, and special category data[1]. By legal basis, we mean the legal reason an organisation has to hold and use personal data[2]. Sharing personal data with others is covered by both the Data Protection Act 1998 and the common law (we provide guidance on the common law in sections 4 and 5).

The UK parliament will further define which legal bases will be available to organisations in the Data Protection Bill (DP Bill). Once passed by Parliament, the DP Bill will become our new Data Protection Act and, alongside GDPR, will form the new UK data protection legislation. We are working with the HRA to produce guidance on the new legislation, which will be released as soon as possible.

In the meantime, this guidance will help DPOs as well as Research Governance managers, researchers, etc. to clarify:

- which legal basis they are most likely to be using (under the current law) to hold and use personal data to support research. The transition to GDPR will be much easier if you are aware what your current legal basis is under the Data Protection Act 1998; and
- the difference between data protection and the common law duty of confidence (the duty of confidence will not change when GDPR is implemented). Again, understanding this distinction will help you interpret the interaction between the common law and the coming new legislation.

[1] Special category data in GDPR is largely equivalent to sensitive personal data under the Data Protection Act 1998 (DPA), with the addition of identifying biometric and genomic data.
[2] The DPA describes the holding, collating, archiving, analysing or using data in any other way, as 'processing'.

1. Legal Basis – personal data (Data Protection Act 1998 (DPA))

The DPA allows organisations to hold and use personal data if they have a legal reason to do so (i.e. if they have a legal basis). Organisations do not currently have to be explicit about which legal bases they are using. As a result, although most organisations will have a legal basis to hold and use personal data, they may not have explicitly indicated what this is.

The legally acceptable reasons for holding personal data are currently defined in the DPA, and listed in the Appendix to this guidance. Schedule 2 conditions apply to all personal data and additional conditions (listed in schedule 3) apply to sensitive personal data. These are the legal bases available under the DPA.

The intention of the DPA was to allow organisations that need to hold and use personal data to support their legitimate activities, to do so.

As such, schedule 2 of the DPA provides the legal basis of supporting **processing 'necessary for the purposes of legitimate interests'**, where that processing is 'not unwarranted because of prejudice to the rights and freedoms of the data subject' (in other words, provided that you are fair to the individuals whose data you are holding (see below)).

Research is a legitimate activity conducted by many organisations (e.g. universities, NHS, a variety of research charities, commercial companies, etc.). Therefore where research requires the use of **personal data**, these organisations are likely to be using **legitimate interests** as their legal basis (under the DPA).

The DPA demands that organisations are also **fair**[3] about how they hold and use personal data. That is organisations:

1. have made available information, describing the personal data they are holding, and what they are doing with it, and they
2. continue to hold and use personal data only if people do not object. The DPA provides individuals with a limited right to object. This ensures that critical legitimate activities do not become impossible for organisations to carry out if individuals were to object to the use of their personal data. Offering an appropriate right to object also helps you ensure that you are being fair (see below).

2. Further conditions – sensitive personal data (Data Protection Act 1998 (DPA))

Most medical research uses **sensitive** personal data (see guidance note 1).

Research organisations that hold sensitive personal data must ensure they have a legal basis to hold personal data (section 1 above), and they must meet one of the additional conditions in schedule 3 of the DPA. You can find a list of these additional, schedule 3 conditions in the Appendix.

[3] Definition of 'fair' is provided in the ICO guide 'Guide to data protection'

Schedule 3 allows organisations to hold and use **sensitive** personal data when it is '**necessary for medical purposes'**. Medical research is considered to be a 'medical purpose' in the DPA. 'Medical purposes' also includes treating patients, managing the NHS, teaching medical and nursing staff etc. The word 'necessary' implies that the research would be impossible without sensitive personal data.

It is likely that most universities, NHS organisations, medical research charities etc. hold and use **sensitive personal data** for medical research with **'legitimate interest'** as their legal basis under schedule 2, and **'necessary for medical purposes'** as their schedule 3 condition (under the DPA).

3. Consent and the Data Protection Act 1998 (DPA)

We have not yet mentioned consent in this guidance. Consent is very important in research. Yet, consent is (in most cases) not likely to be the **legal basis** allowing research organisations to hold personal or sensitive personal data under the DPA.

Informed, voluntary and fair consent is the cornerstone of ethical research involving people. It is central to ensuring the rights of individual participants can be respected. Researchers holding and using data should always ensure that whenever possible, they seek appropriate consent from the individuals involved. Consent should include: informing potential participants of what types of data you wish to collect, what you intend to do with the data, as well as a description of the risks that might be involved and an idea of how you intend to manage these risks. (See HRA/MRC Consent and participant information sheet preparation guidance).

Although the DPA does not demand that consent is in place for research, other parts of the law do (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.

Consent can help organisations use personal data 'fairly'. Appropriate research consent is a robust mechanism for researchers to ensure they are transparent about what personal data they collect and use, and the risks that might be involved. However, the Information Commissioner's Office suggests that we should never rely solely on consent to ensure 'fairness'. Organisations also need to provide adequate and accessible 'fair processing information' in a privacy notice (e.g. on your website, and in leaflets/posters available in public spaces etc.) and ensure the individuals' limited right to object is respected. That is why we encouraged you to look at consent and all of the other transparency information that your organisation currently provides in our previous guidance note.

The DPA does provide the legal basis of 'consent' to hold and use personal data (schedule 2); and 'explicit consent' as an additional condition for sensitive personal data (schedule 3). However, we envisage that for most research organisations, medical research is such an integral part of what they do, that they can rely on **legitimate interest** (schedule 2) and **necessary for medical purposes** (schedule 3) to hold and use sensitive personal data.

Research is managed tightly within universities, NHS, charities, etc. through governance mechanisms. These governance arrangements should provide research participants with assurance that their personal data is only being used to support legitimate activities (and, in the case of sensitive personal data, is necessary).

4. Common law - confidentiality

The law around information about people is further complicated in the UK. We must also comply with the common law, as it applies to all confidential information. 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 common law duty of confidentiality will not be affected by the implementation of GDPR.

Information is considered confidential in law if:

- It is not in the public domain *(no such limit is placed on the definition of personal data)*, and
- 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 has a degree of sensitivity associated with it (*no such element in the definition of personal data, but there is a similar consideration for sensitive personal data)*, and
- It is given with the expectation that it will be kept confidential. Individuals do not have to be explicit, when entrusting others with their information, that they intend it to be kept confidential. 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 information in line with '**reasonable expectations'**. In other words, confidential information should only be shared when there would be '**no surprises'** for the individuals concerned, unless there is another legal avenue which allows lawful disclosure (see section 5 below).

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 working as part of the interdisciplinary team. In such circumstances, patients would not be surprised if all of their care team, including researchers, were party to their confidential information. However, not all researchers will have this relationship with patients[4].

We know that most people do not understand how research works on the ground. They do not realise that collaboration is common and that data may be shared as

[4] Sections 3.6 and 3.7 of Information to share or not to share: The Information Governance Review.

part of collaboration. You can manage research participants' expectations by informing them if you intend to share their confidential information with others, and to ask them if they are prepared to consent to 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.

Another legal avenue for sharing information is to ensure that it is robustly anonymised[5]. (Information has to be identifiable to be subject to the common law.)

There are times when organisations may wish to share confidential (by definition identifiable) information when sharing is not in line with individuals' expectations. In certain situations, for example to prevent a crime from being committed, common law allows sharing. In such cases, disclosing the information rather than keeping it confidential, best serves the public interest.

5. Disclosure to support research – outside reasonable expectations

In the UK there are other legal avenues that allow the disclosure of confidential information to support medical research, even when this is not in line with 'reasonable expectations'.

In England and Wales, such disclosure can be approved by the HRA Confidentiality Advisory Group (so called 'Section 251 approval'), 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 HSC Privacy Advisory Committee.

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

1. have a legal basis to hold and use personal data (most likely to be **legitimate interest** under the Data Protection Act 1998), and
2. if applicable, comply with a condition that allows them to hold sensitive personal data (most likely to be **necessary for medical purposes** under the Data Protection Act 1998), and
3. be **fair** about how they hold and use this data (organisations must have made an appropriate privacy notice available and be able to respect individuals' limited right to object. (Be aware that when HRA CAG approves disclosure, they require researchers to provide additional notification to the relevant patient population, so called 'patient notification').

[5] ICO Anonymisation Code for further guidance.

6. Putting it all together

Consent is at the heart of ethical research. Consent can help ensure that data is transparently held and used for research (helping organisations to act **fairly**, as required by the Data Protection Act 1998. 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.

The Data Protection Act 1998 (DPA) does not demand consent (explicit or otherwise) to be in place to hold and use personal data (including sensitive personal data). Organisations must have a **legal basis** to hold and use personal data and ensure that individuals are treated **fairly**. The most likely legal basis used by research organisations to hold and use personal data under the DPA is **legitimate interests**; with the additional condition of **necessary for medical purposes** if they hold sensitive personal data.

Once organisations are holding personal data legally and fairly, they must comply with the rest of the DPA (for further requirements see Using information about people in health research).

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).

Appendix

Data Protection Act 1998

SCHEDULE 2

Conditions relevant for purposes of the first principle: processing of any personal data

1. The data subject has given his consent to the processing.

2. The processing is necessary—

   (a) for the performance of a contract to which the data subject is a party, or

   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary—

   (a) for the administration of justice,

   (b) for the exercise of any functions conferred on any person by or under any enactment,

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. —(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

   (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Data Protection Act 1998

SCHEDULE 3

Conditions relevant for purposes of the first principle: processing of sensitive personal data

1. The data subject has given his explicit consent to the processing of the personal data.

2. —(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

   (2) The Secretary of State may by order—

   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

   (b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—

   (a) in order to protect the vital interests of the data subject or another person, in a case where—

      (i) consent cannot be given by or on behalf of the data subject, or

      (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—

   (a) is carried out in the course of its legitimate activities by any body or association which—

      (i) is not established or conducted for profit, and

      (ii) exists for political, philosophical, religious or trade-union purposes,

   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

   (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—

   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

   (b) is necessary for the purpose of obtaining legal advice, or

   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. —(1) The processing is necessary—

   (a) for the administration of justice,

   (b) for the exercise of any functions conferred on any person by or under an enactment, or

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

   (2) The Secretary of State may by order—
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. —(1) The processing is necessary for medical purposes and is undertaken by—
   (a) a health professional, or

   (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

   (2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. —(1) The processing—

   (a) is of sensitive personal data consisting of information as to racial or ethnic origin,

   (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

   (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

   (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.