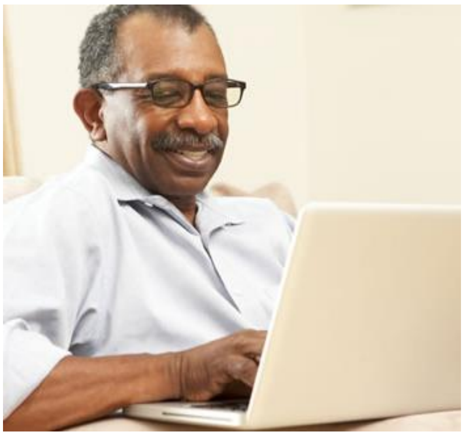
MRC | Medical Research Council

MRC ethics series

Using information about people in health research



Medical Research Council
Version 2.0, June 2018

This guidance is updated by the MRC Regulatory Support Centre. It does not reflect requirements of the General Data Protection Regulation (GDPR) – further details on how data protection law applies to research can be found in our GDPR Resources.

Foreword

Welcome to the Medical Research Council's guide on using information about people in health research.

Information about people is fundamental to health research. This guide applies to research using any type of information about people. The principles and guidance outlined here are designed for all MRC employees and reflect best practice for MRC-funded researchers.

The General Data Protection Regulation (GDPR) and the UK Data Protection Act came into force on 25th May 2018. Together these laws have some additional requirements which are not yet adequately covered within this guidance (see Summary of relevant law below or our GDPR resources[1] for further details). This guide was produced by the MRC Regulatory Support Centre[2] in conjunction with experts in the field (available from Acknowledgments below) and replaces the 2001 MRC publication Personal Information in Medical Research.

This guide has been released for consultation in use. If you have any comments to feed back about this guidance, then please contact the MRC Regulatory Support Centre at rsc@mrc.ukri.org.

Note on identifiability: Protecting people's privacy is important. Previous practice in the UK has often relied on the removal of identifiers as a way of maintaining confidentiality. This guide recognises that we live in an age where an increasing amount of data relating to individuals is in the public domain. This brings with it an increased risk of (re)identification for any individual level data. We therefore acknowledge that obtaining complete anonymity, when using individual level data, may be difficult to achieve if datasets are to remain useful for research. However, data can be sufficiently anonymised to satisfy particular legal thresholds and protect individual privacy where specific additional controls are in place (e.g. Data Transfer Agreements, Data Sharing Agreements, or similar). We believe that managing the risk of (re)identification is fundamental to balancing privacy and conducting research, and we highlight resources which describe how to do this (Information Commissioner's Office Anonymisation Code of Practice[3] and UK Anonymisation Network decision-making framework)[4].).

Related links

1. MRC Regulatory Support Centre, GDPR resources **https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/gdpr-resources/**
2. MRC Regulatory Support Centre **https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/**
3. Information Commissioner's Office (ICO) Guide to data protection, Anonymisation (with links to the Anonymisation Code of Practice) **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**
4. UK Anonymisation Network decision-making framework **http://ukanon.net/ukan-resources/ukan-decision-making-framework/**

Contents

This guidance is updated by the MRC Regulatory Support Centre. It does not reflect requirements of the General Data Protection Regulation (GDPR) – further details on how data protection law applies to research can be found in our GDPR Resources.

This guidance is updated by the MRC Regulatory Support Centre. It does not reflect requirements of the General Data Protection Regulation (GDPR) – further details on how data protection law applies to research can be found in our GDPR Resources.

1. Principles

This section summarises the key principles that should be followed when collecting and using information about people in the course of health research.

1 **Fairness and respect** - Information of any sort which is provided for health care, or obtained in health research, must be treated with respect and used fairly. Researchers and/or their organisations must inform people how information about them is to be used to support research. This should be done in a way that is accessible to the individuals whose information is to be used (i.e. accessible both in terms of how easy it is to understand and how readily available it is). There should also be a fair opportunity for the individuals concerned to have a say in how their information will be used. Explicit consent is the usual route for using identifiable information about an individual in health research but other legal routes exist.

2 **Demonstrating trustworthiness** - Health research is dependent upon the use of information about the health, social status and other aspects of people's lives. It is vital that all those who handle such information for research do so in a manner that demonstrates trustworthiness to maintain the confidence of participants and the population as a whole. As part of this, researchers must keep up to date with all ethical, regulatory and governance requirements relating to the use of information about people for research.

3 **Benefits versus risks** - Research should only go ahead if the potential benefits of that research, outweigh any potential risks to participants. The risks to privacy and confidentiality must be fully considered before research begins. Risks should be assessed and well-managed (i.e. appropriate risk mitigation measures must be put in place and risk monitored throughout the research process).

4 **Ethical review** - All health research involving 'identifiable information' must be approved by a Research Ethics Committee.

5 **Minimise use of identifiable information** - Researchers should always consider the information needed to address their research question and personal identifiers must only be held for research when this is necessary for the conduct of the study.

6 **Limit access to identifiable information** - Principal Investigators must take responsibility for ensuring that personal identifiers are separated from the research data as early as possible and are only shared within the research team on a need to know basis. Even information capable of indirectly identifying an individual should have controls in place to minimise the risk of (re)identification.[*]

Before sharing identifiable information with a member of their team, Principal Investigators must ensure that the person is trained and competent to handle the information in an appropriate manner and understands their responsibility for protecting confidentiality.

7 **Ensure security and validity of research data** - Principal Investigators must ensure that appropriate systems or processes are in place to protect the integrity and security of research data throughout the research process from collection, transcription, analysis, to publishing, sharing and archiving. Much of this is a corporate responsibility and so it is important that Principal Investigators work within local information security policies and with relevant experts.

[*] If the risk of (re)identification is *sufficiently* mitigated to the point of becoming a remote risk, then data may satisfy the ICO Anonymisation Code of Practice. In this case the data may not, while in this controlled environment, be considered identifiable (either directly or indirectly). For more on identifiability see Anonymisation and pseudonymisation.

8 Decisions about disclosures must be well informed - Any decisions made about sharing information relating to an individual research participant must be made after consideration of their expectations, relevant policies and the law (particularly concerning the risk of (re)identification).

9 Data sharing and publishing - Principal Investigators must ensure that all research findings are put in the public domain and, when appropriate, primary research data are made available for further research in a manner consistent with these principles and the law. Research participants should be made aware that their data may be shared with others. This should include details of the controls and limitations placed upon these data to protect their privacy.

10 Feedback of results - At the outset, researchers must decide how and when research results will be made available to participants. Researchers should also plan if any personal feedback will be provided to research participants about possible health related findings[1]. When appropriate these plans should be agreed with a Research Ethics Committee. Researchers must be prepared to reconsider these plans in light of unforeseen findings and discuss the appropriate response with a Research Ethics Committee.

Related links

1. MRC and Wellcome Trust Framework on the feedback of health-related findings in research **https://mrc.ukri.org/documents/pdf/mrc-wellcome-trust-framework-on-the-feedback-of-health-related-findings-in-researchpdf/**

This guidance is updated by the MRC Regulatory Support Centre. It does not reflect requirements of the General Data Protection Regulation (GDPR) – further details on how data protection law applies to research can be found in our GDPR Resources.

2. Summary of relevant law

When using information about people in health research in the UK, you need to be aware of the legal framework and how this might impact on what you intend to do. This summary does not attempt to cover every aspect of the law but focuses on requirements for those who are directly involved in the delivery of health research (e.g. researchers, data managers, research nurses, etc.). **This summary does not reflect the requirements of current data protection law. For further information please visit General Data Protection Regulation (GDPR) below.** If you are responsible for ensuring the security, validity and/or integrity of data (e.g. Information services / Information technology specialists, Data Protection Officers etc.), then there are additional requirements which you will need to meet. For further guidance please visit the Information Commissioner's Office (ICO) website[1].

Common Law of Confidentiality

Common law governs the use of confidential information in research. Be aware that the requirement to comply with the common law of confidentiality **was not** affected by the implementation of the UK Data Protection Act and GDPR.

You owe a duty of confidence when you know information about an identifiable individual and they have a reasonable expectation of privacy with respect to that information (e.g. patient and doctor). The courts suggest that this reasonable expectation be judged objectively and by reference to the **reasonable person of ordinary sensibilities**.

If information is provided to you with the understanding that it will not be revealed to anyone (other than to those that the individual might reasonably expect in the circumstances), then you must respect this 'duty of confidence' (e.g. only disclosing confidential information with consent or strong justification – see Accessing identifiable information without consent below).

Holding information under a duty of confidence is not the same as a keeping a secret and disclosing confidential information does not necessarily breach a duty of confidence. Take the example of a patient who visits their GP to discuss symptoms which could be due to cancer. During the consultation the GP may suggest referring the patient for further tests. Following such a consultation, the patient would not be surprised to receive an appointment letter from a hospital inviting them to attend for testing. This concept of the GP sharing the patient's information in order to ensure continuity of care (i.e. sharing information within the 'care team') does not breach patient confidentiality. The patient has an expectation that the GP will share information with relevant colleagues in both the GP practice and the hospital in order to provide them with access to the appropriate health care services (i.e. the patient's consent is implicit). Whether this expectation extends to research will depend upon the conversation that took place between the GP and the patient and/or any other information about the use of patient data in research provided to patients.

Even if you have access to patient health data because you are part of the care team, you should only share this information for research in line with the individual patient's expectations. If your intention is to disclose confidential information for the purposes of research outside of the care team, then this must be done with the patient's explicit consent or through another legal avenue.

Where researchers have direct contact with participants for the purposes of health research, a duty of confidence is established between the participant and the researcher. Participants should be made aware of the limits of this duty (e.g. that their information will be shared with a wider research team). This understanding cannot be assumed since the general public are not familiar with how research works in practice. When researchers intend to share information outside of the wider research team, participants should be informed of this - see also Data sharing and publishing. There should be no surprises for participants in terms of how their information will be shared for the purposes of health research.

Health and social/community care services in the UK protect patient confidentiality and the use of confidential patient information through Caldicott Guardians. A Caldicott Guardian is a senior person within an NHS organisation responsible for protecting the confidentiality and enabling appropriate sharing of confidential patient information. Caldicott Guardians play a key role in ensuring that NHS, councils with social services responsibilities and partner organisations follow the Caldicott Principles[2] for handling confidential patient information.

Usually it is in the public interest to maintain any duty of confidence. There are however occasions where disclosure of information might be seen to be in the public interest or is required by law. In England and Wales this has to be in the overwhelming public interest for example:

- Safeguarding children or vulnerable adults where there is a suspicion of abuse / negligence; or
- A requirement for the notification of infectious diseases (NOIDs) and reportable causative organisms.

In Scotland interpretation of confidentiality law allows the disclosure of confidential patient information to support good quality research when this is deemed to be in the public interest. In England and Wales, there is a permissive statutory gateway enabling the disclosure under Section 251 of the NHS Act 2006. Northern Ireland also have a legal avenue. (For more, see Accessing identifiable information without consent below).

Release of ‘anonymised data’ does not constitute a breach of confidence where the risk of (re)identifying an individual is sufficiently mitigated. For more guidance select Anonymisation and pseudonymisation.

It should be noted that a duty of confidence extends after death.

Accessing identifiable information without consent

When consent is not possible or is impractical, the law allows disclosure in certain circumstances. In England and Wales, Section 251 of the NHS Act 2006, and subsequent Regulations (‘COPI regs’), allows for the Common Law of Confidentiality (see above) to be set aside temporarily for defined medical purposes. This allows time-limited disclosure of ‘confidential patient information’, without patient consent, for medical research. Section 251 should only be considered as a last resort, when all other options have been exhausted.

The Health Research Authority Confidentiality Advisory Group (HRA CAG) provide independent advice on the use of Section 251. HRA CAG are required to consider:

- Whether the use of the information will improve patient care or if it is otherwise in the public interest.
- If the purpose of the study can be achieved without breaching confidence. In particular:
  - Would it be practicable to obtain consent for use of confidential patient information?
  - Could researchers receive and use data in an appropriately anonymised form?
  - Can necessary linkages with confidential patient information be performed by others who may already hold data in identifiable form, e.g. NHS Digital?
- Whether there are adequate security arrangements in place to limit further disclosure (achieved in England through the applicant’s annual completion of the NHS Data Security and Protection Toolkit[3]; Wales has an equivalent system[4]).

HRA CAG also look to applicants to demonstrate:

1. Adequate notification of the intended research to the relevant population. This will typically involve publishing details of the research together with information on how to opt-out, somewhere that it can be read by those whose data may be used. (HRA CAG may refer to this responsibility as patient notification).
2. A clear process for recording and handling those who object to data about them being used for research.

Section 251 cannot set aside Data Protection Act responsibilities (e.g. the need to be ‘lawful, fair and transparent’).

An application may be excluded from Section 251 support if researchers have attempted to contact potential participants about consent and received no response. ICO deems non response in such circumstances as ‘refusal to consent’ since the first data protection principle (that data be processed ‘fairly and lawfully’) could not be satisfied in relation to ongoing processing. For more please see the HRA's guidance on managing non-response[5].

It should be noted that Section 251 approval is a permissive approval. Even when a researcher has successfully obtained Section 251 approval, this does not mandate that a Caldicott Guardian within an NHS organisation provide the researcher with the required confidential patient information. Please see the HRA CAG webpages[6] for further guidance on Section 251 approval and how to apply.

Although not enabled through legislation, the ‘duty of confidence’ can be set aside in Scotland when this is in the public interest. Access to confidential information within one NHS board in Scotland can be sought from the local Caldicott Guardian. Access to confidential information in more than one NHS board in Scotland or from the Information Services Division (ISD) requires application to the Public Benefits and Privacy Panel (PBPP)[7] who review requests to use NHS Scotland-controlled data and/or the NHS Central Register data for health and social care research. Successful applicants are required to demonstrate that they have completed appropriate training (e.g. SURE training) and must sign up to the conditions of an end-user agreement.

In Northern Ireland the Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016 provides the legal basis for setting aside the duty of confidence. The Act applies to the confidential information of patients and/or social care service users in Northern Ireland and includes use in health and social care research.

For further details please see Working without consent.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 were implemented on the 25th May 2018. These two pieces of legislation currently form data protection law in the UK. They provide data protection rules for ‘personal data’ which more adequately support the rights of the individual in the digital age. The requirements support research, much of which reflects current good research practice.

It is worth noting that whilst many requirements of the 2018 law are similar to the old Data Protection Act, there are some additional requirements. Among other things, the first principle is now ‘lawful, fair and transparent’ so importance on informing participants (transparency) has increased. There’s also the new ‘accountability’ principle which increases the responsibility of organisational Data Protection Officers (DPOs). Your DPO is a key contact in helping you meet requirements of data protection law.

The additional requirements are not yet adequately covered within this guidance. However, you can find further detail on the MRC Regulatory Support Centre’s GDPR resources[8]. The Information Commissioner’s Office[9] also provides generic guidance for all organisations holding and using personal data (which is not necessarily research specific).

Throughout this guidance we use the term ‘consent’ or ‘explicit consent’ to mean consent to take part in research or consent in line with **reasonable expectations** to manage the disclosure of confidential information under common law. We do not mean consent or explicit consent as defined in GDPR (i.e. consent as the ‘lawful basis’ for ‘processing’ personal data). The most appropriate lawful basis for processing personal data in research is either 'task in the public interest' for public authorities like universities and research council institutes; or 'legitimate interest' for charity research organisations.

Related links

1. Information Commissioner's Office (ICO) website guidance on security **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/**
2. Department of Health, Information: To Share or not to Share Government Response to the Caldicott Review, September 2013 **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF**
3. NHS Data Security and Protection Toolkit (replaces the NHS Information Governance Toolkit) **https://www.dsptoolkit.nhs.uk/**
4. NHS Wales Informatics Service, Information Governance and Caldicott (with links to the Welsh IG Toolkit for GMPs) **http://www.wales.nhs.uk/sites3/home.cfm?orgid=950**
5. Health Research Authority (HRA), Managing non-response: establishing the ICO and CAG position **https://www.hra.nhs.uk/documents/258/managing-non-response-guidance-v1-2.pdf**
6. HRA, Section 251 and the Confidentiality Advisory Group (CAG) **https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/**
7. The Scottish Government, Information Governance (with links to the Public Benefit & Privacy Panel (PBPP) website) **http://www.informationgovernance.scot.nhs.uk/**
8. MRC Regulatory Support Centre, GDPR Resources **https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/gdpr-resources/**
9. ICO GDPR guidance **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/**

3. Identifying potential participants

Before you can start your research, you may need to find specific types of potential participants, in order to ask them for their consent to take part in your study.

For example:

- Patients with tumours that have or have not responded to a specific treatment
- People with type II diabetes with either good or bad glycaemic control
- Patients with a rare condition who could potentially present at any hospital in the UK
- People born within a specific period of time and within defined postcode areas

When identifying potential participants for research you need to ensure that any disclosure of confidential information is lawful. For more please see Common Law of Confidentiality and Accessing identifiable information without consent. GDPR also applies (e.g. you need to be lawful, fair and transparent).

You are part of the care team

You can access your patients' confidential information directly to identify them as a potential research participant without breaching confidentiality if you are part of the 'care team'. You should also ensure that your organisation's 'privacy notice' includes the potential use of patient data for research.

An NHS honorary research contract does not in itself qualify you to be part of the patient's care team. However, researchers with a clinical role are often embedded within multidisciplinary care teams and as such have a 'legitimate relationship' with their patients and the right to access confidential information about them. For a more detailed definition of the care team and whom this may or may not include please see Sections 3.6 and 3.7 of Information to share or not to share: The Information Governance Review[1].

If you do have the right to access confidential information about your patients, you should not pass this on to others unless your patients would expect this (e.g. with explicit consent). The patient might well be surprised if confidential information about them was disclosed to someone outside the care team, with whom they have no legitimate relationship.

With explicit consent

You can disclose confidential information for the purposes of research with the consent of the individual to whom the information relates - see also Consent to approach lists (under the section Other possible solutions for identifying potential participants below). Whenever practicable you should seek consent from potential participants to use their information in your research.

If you are not part of the 'care team' and you need confidential information about patients for the purposes of your research, then you will either need to:

- identify someone who does have a 'legitimate relationship' with these patients to help you with recruitment (i.e. by asking them to make the initial approach and then either seeking consent on your behalf or inviting participants to respond to you); or
- you must explore other legal avenues.

Researchers need a legal avenue to access any confidential information, including:

- confidential information held outside of the health and social / community care services in the UK (i.e. non-NHS). This might include confidential information held by other government agencies, such as HM Revenues & Customs etc.; and/or
- confidential information held by other research teams e.g. academic collaborators etc.

Participant recruitment with support from those who have a legitimate right to access confidential information is often the most appropriate route, provided this does not breach any duty of confidence – for further details please see the Common Law of Confidentiality (available from **Summary of Relevant law**).

Through other legal avenues

There are circumstances when confidential information can be legally and ethically disclosed to those with no established duty of confidence – see Working without consent.

Using registration data

It may be possible to identify potential participants by accessing existing identifiable data from other sources - see Accessing central NHS and other government data.

These sources can also provide access to existing 'anonymous data' and/or 'anonymised data'. You should always first consider the use of anonymous or anonymised data and whether this is suitable for your research – see Use of an anonymised dataset (under the section Other possible solutions for identifying potential participants below).

Other possible solutions for identifying potential participants

Use of an anonymised dataset

Do you need confidential information in order to identify potential participants? If you do not need to access information which will identify your individual research participants (e.g. you do not need to contact them directly, nor need their personal identifiers for the purposes of your research) then you should use 'anonymised data' created by the organisation which has a legitimate right to access your potential participants information (e.g. an NHS organisation, NHS Digital, academic collaborator etc.).

Researchers, health professionals and managers need to work together to use information technology and infrastructure to reduce dependence on disclosures of confidential information without consent, whilst facilitating records-based research. The implementation of electronic records within the NHS, offers researchers improved access to anonymised data about patients whilst facilitating complex data linkage.

Advertising for potential participants

Would a poster in a GP or clinic waiting room (with permission), an advert in a local paper or on local radio and/or promoting your research via social media be effective means of identifying potential participants for your research? If so you may wish to explore these methods of indirect recruitment rather than asking either members of the 'care team' or academic collaborators to help you with recruitment. If potential participants identify themselves to you then there will be no breach in confidentiality and you can then ask them to consent to your research.

This can work in some circumstances but is often not as effective as targeted recruitment.

Using trustworthy environments

Trustworthy environments (sometimes referred to as safe havens or safe environments) offer researchers secure access to confidential information for linkage and analysis. Access within these secure and controlled environments is only provided when researchers can fulfil strict application criteria. Trustworthy environments can also provide access to anonymised data created by specialist staff using technical solutions such as indexing, data linkage etc. This allows researchers to analyse linked individual participant level data whilst maintaining the confidentiality of the individuals to whom the information relates. Please see the Administrative Data Research Network[2] for a list of UK resources.

Consent to approach lists

A number of research active organisations have begun to use consent to approach lists, as a means to identify potential participants. Potential participants should be informed of the consequences, in the short and long-term, of being on these lists.

Such lists must be kept up to date to ensure that contact details remain valid over the lifetime of the list. Research active organisations running consent to approach lists should seek consent from those on the list to either:

1. be in regular contact; or
2. check contact details are up to date with other organisations (such as NHS Digital in England and Wales or the Information Services Division in Scotland).

Using non-health sources to contact people

Direct approaches to members of the public identified from the electoral roll or other public sources do not require consent or the agreement of the individual's doctor, but it is usually advisable to notify local GP Practices before carrying out a study in their area. Email or postal approaches are generally less likely to lead to distress or misunderstanding than cold telephone calls.

Selection according to community or group

If your research focuses on the health of distinct communities or groups e.g. due to race or ethnicity, socio-economic status, disability, etc. then you should consider whether community organisations or other bodies should be made aware of the study. Such organisations or bodies might be able to represent the interests of such groups who should have the opportunity of commenting on the research. When identifying potential participants in this way, the law still applies and any access to confidential information must not breach any duty of confidence. For further details please see the Common Law of Confidentiality (available from **Summary of Relevant law**).

Selection by employment

Occupational surveys to assess risks from work activities, accidents or from exposure to particular hazards or toxic substances are often based on employers' records. Prior to such a survey, discussions should take place with representatives of the staff involved, with management, the occupational health service, and where possible with the staff themselves. A normal approach to individuals would be through a letter confirming that the employer and the Trade Union agreed to the study taking place. Again, when identifying potential participants in this way, access to any confidential information must meet the Common Law of Confidentiality. Publicity through a newsletter, etc. should also be considered, depending on the sensitivity of the issue being studied.

Related links

1. Dame Fiona Caldicott, Information: To share or not to share? The Information Governance Review, March 2013 **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf**
2. Administrative Data Research Network, Get Data, Secure facilities in the UK **https://www.adruk.org/our-data/our-data-services/**

4. Collecting data and consent

Collecting data for research may involve participants directly or may occur through access to data resources held elsewhere.

For example:

- Participants recruited to a study, consent is taken and data (and tissue samples) are collected
- Data are collected directly from a person's medical notes, there is no direct contact with any participant
- Data are obtained from another research group, there is no direct contact with any participant
- Data are obtained from NHS central information or other government sources, there is some direct contact with participants
- Data are obtained from NHS central information or other government sources, there is no direct contact with participants

When collecting data for research you need to be aware of the legal framework. Please see **Summary of relevant law** for further guidance.

Before collecting data, you must assess whether obtaining consent to use data about people in these situations is practicable, or could be made so, and to base research on explicit consent whenever possible:

- Where a study does not require direct contact with participants, this should not in itself be a reason not to seek consent
- Decisions relating to practicability may consider attributes of the study population, the research and whether bias may be introduced by seeking consent
- You should be aware that in some circumstances other legal frameworks may demand consent to be in place before research can begin (e.g. to conduct a clinical trial of an investigational medicinal product and comply with The Medicines for Human Use (Clinical Trials) Regulations 2004, or to collect and use tissue for research where no exemption applies to the consent requirement of the Human Tissue Act 2004, etc.). The Health Research Authority (HRA) provide detailed guidance on consent.

Obtaining explicit consent

Explicit consent requires an explicit act, affirmed in a clear statement (e.g. an individual's verbal or written agreement to take part in research). Explicit consent requires you to explain your research and what taking part would mean for potential participants. This will include providing adequate information to potential research participants in a form that they can understand.

Consent can only be considered valid if it is given freely, if the person is competent to make the decision and the decision is made having been appropriately informed. For further guidance on seeking consent from groups who may lack competence, please see the MRC Ethics Series[1] (in particular guidance on adults who cannot consent and children).

In a health research context, consent can be broad in both time and scope. For example, a potential participant may be asked to consent to a specific research study as well being informed that their data may be shared in future research. (If the intention is to share identifiable data for future research, potential participants should be asked for explicit consent to do this.) It can be difficult to know the exact purposes to which data may be put in the future. However, this inability should not prevent you from trying to be as specific as you can about these potential future uses in your own particular circumstances.

During the consent process, participants should be informed of what data you intend to collect about them, how it will be kept secure and which organisation will be responsible for keeping it safe, as well as your long-term plans for sharing, archiving and publishing their data.

Very occasionally it may be necessary to publish identifiable data about an individual participant for the purposes of your research (e.g. if it includes certain phenotypic traits, rare diseases or statistical outliers). In these cases, there should be a dialogue with the individual(s) involved to explain exactly what will be published including any measures that you will take to mitigate the risk of their identification (e.g. covering their eyes in a photograph, as long as doing so does not compromise the scientific value of the photograph).

Potential participants should understand the implications of taking part in your study, including the medium or long-term implications. For example, future uses of data about them where known, and if not known are participants happy with the unknowns; are you planning to share their data with others, if so, how will their privacy be protected? How will you keep participants updated on the research uses, and will your systems support their choice in how data about them is used?

Explaining how data will be managed and kept safe in lay language can be difficult. Understanding Patient Data[2] has done some work to help standardise terminology when explaining the concept of 'anonymisation' to the public. Every effort should be made to ensure that information provided to participants is understandable and relevant to them. The best way to ensure the information provided is appropriate, is to test it with members of the general public or with groups of potential future participants, and to encourage them to provide feedback on how to improve the information you plan to provide.

Participants should be made aware that they can withdraw their consent from your study. It should be clear to participants what withdrawal will mean and how this will be managed by the research team, e.g. withdrawal from all future analyses, withdrawal from the collection of new data but existing data will remain in the dataset etc. Participants should understand the limits of withdrawal and it should be made clear when withdrawal is no longer possible, e.g. after submission for publication.

You should keep a record of the consent given; including the information provided to participants and the signatures of all those involved in the consent process (participant, researcher and in some circumstances witness, proxy or consultee).

Consent is ongoing and can be revisited over time. Individuals may choose to withdraw consent (discussed above) and while activity is taking place on the basis of consent, then opportunities should be taken to ensure that the consent remains appropriately informed; particularly if circumstances change.

A research ethics committee should review all consent documentation. You must use adequate version control on consent documentation (as well as on all other study documents) so that amendments can be managed effectively as the study progresses and it is clear which version was in use at any particular time.

The HRA provide comprehensive guidance on both legal and ethical frameworks surrounding consent, and details of how to prepare consent documentation in the MRC / HRA Participant Information Sheet guidance[3].

Collecting data through other sources

If you intend to access data from other sources (e.g. through NHS Digital) you should be aware that you will need to satisfy their requirements in terms of consent or find an alternative legal avenue - see also **Accessing central NHS and other government data**.

Collecting data without consent

If consent is not practical and you require a legal avenue to access and collect identifiable information see **Accessing identifiable information without consent.**

Collecting non-identifiable data

If you don't need to collect data that will identify individual research participants (e.g. you don't need to contact them directly, nor need their personal identifiers for the purposes of your research) then collect 'anonymised data'. Collecting robustly anonymised data does not require consent by law. For more please see **Anonymisation and Pseudonymisation**.

Related links

1. MRC Policies and guidance for researchers, MRC Ethics Series **https://mrc.ukri.org/research/policies-and-guidance-for-researchers/#ethics**
2. Understanding Patient Data, New words and pictures to explain anonymisation, 6 April 2017 **https://understandingpatientdata.org.uk/news/new-words-and-pictures-explain-anonymisation**
3. Consent and Participant Information Sheet Preparation Guidance **http://www.hra-decisiontools.org.uk/consent/**

This guidance is updated by the MRC Regulatory Support Centre. It does not reflect requirements of the General Data Protection Regulation (GDPR) – further details on how data protection law applies to research can be found in our GDPR Resources.

5. Anonymisation and pseudonymisation

Reducing the identifiability of data (and thus minimising the risk of (re)identification) is essential to protecting the privacy of research participants and preventing any unintended disclosure of confidential information – see also Common Law of Confidentiality (available from **Summary of Relevant law**). Researchers use a number of methods to routinely do this, such as anonymisation, pseudonymisation, encryption and restricting access via password protection.

This section focuses on 'anonymisation' and 'pseudonymisation' as means to use and share information whilst protecting privacy. Acknowledging that when working with individual participant level data, ensuring complete anonymity can be difficult to achieve without compromising the usefulness of data for research.

What makes information identifiable?

When considering how identifiable information is, you must consider content and context.

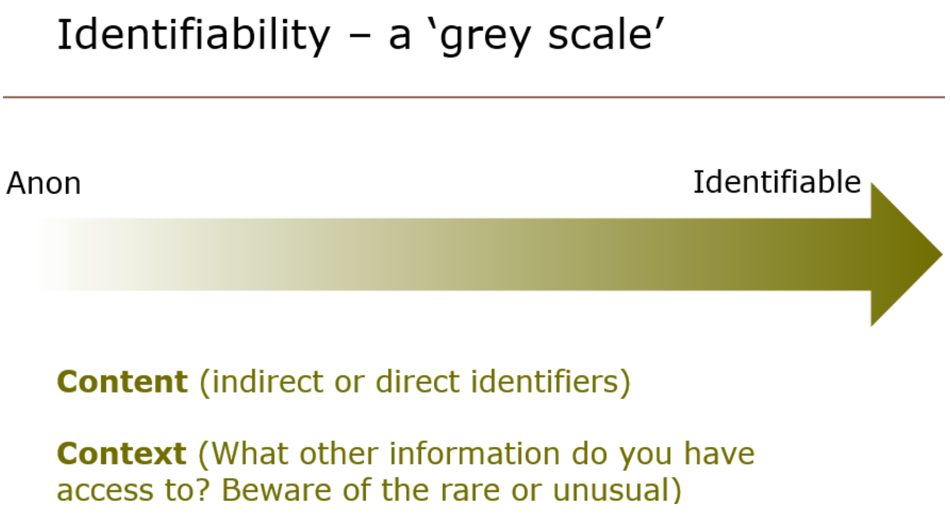
Content of datasets

There are certain pieces of information that can directly identify an individual (direct or personal identifiers); e.g. name, email address, postal address, etc. Other pieces of information, whilst less identifiable on their own, become more identifiable when used in combination with other pieces of information or held in contexts where they can be associated with direct identifiers e.g. NHS number, date of death etc.

The context

The context in which information is processed greatly affects how identifiable it is. In one context (small geographical area with low population numbers, a rare disease or a rare occupation for example) even indirect identifiers become much more identifiable than the same data items viewed in other circumstances. Another important element of context is the availability of other information (either in the public domain or within your organisation) that might combine to increase the risk of identification of individuals. You can limit access to identifiable information within your research team by working to established rules (e.g. storing personal identifiers in locked filing cabinets or on restricted access network folders which only a limited number of the team can access).

In reality there exists a continuous scale of identifiability, as illustrated in image below:


Identifiability – a 'grey scale'
Anon
Identifiable
Content (indirect or direct identifiers)
Context (What other information do you have access to? Beware of the rare or unusual)

Ways to reduce identifiability

In practice however you need to consider whether information is identifiable or not in order to make appropriate decisions about how you will use and share data in compliance with the law. Please select **Summary of relevant law** for more information.

Some data can be considered inherently 'anonymous' as no individual can be identified either directly or indirectly (by putting it together with other information). This describes most aggregate data.

It is acknowledged that removing all risk of (re)identification may be difficult to achieve, if not impossible, particularly where data continues to be held at individual participant level.

'Anonymised data' does not identify an individual directly and is unlikely to allow (re)identification in combination with other data. To ensure this you must mitigate the risk of (re)identification until it is no longer reasonably likely (e.g. by controlling the risk of (re)identification through the use of legal agreements which robustly control the context within which the information is viewed). For further guidance please see the ICO Anonymisation code of practice[1].

It is common practice when collecting information for research to pseudonymise it very early in the research process. Pseudonymised and anonymised data are not the same. The difference between them is the level of control preventing (re)identification. Although both involve a physical separation of personal identifiers from the rest of the dataset, in the case of 'pseudonymised data' the decryption key or cipher is kept within the same organisation (i.e. the 'Data Controller') as the rest of the dataset.

Pseudonymised data are classed as 'personal data' whereas anonymised data are not. One reason to use pseudonymised data is to limit the risk of accidental or unintentional disclosure by minimising how many people have access to identifiable information and to provide additional protection.

Some identifiers can be changed to even less identifiable parameters: e.g. date of birth changed to age; postcode changed to part of postcode or social deprivation score etc. Care should be taken with embedded, machine generated identifiers on scans or images produced within the NHS or excess diagnostic samples which will be labelled with personal identifiers for the purposes of diagnosis. These should be anonymised or re-labelled for research use before they are disclosed.

Anonymisation is in itself a science. The extent of anonymisation / pseudonymisation can often be a difficult decision. This decision should be made by the Principal Investigator with support from the ICO's Anonymisation Code, the UK Anonymisation Network decision-making framework[2], and local Data Protection colleagues (e.g. the organisation's Data Protection Officer or equivalent).

Collection and collation of information

When planning your research you should ask yourself whether the use of 'identifiable information' is necessary (as the law does not place restrictions on the use of ''anonymised data''). Personal identifiers should only be kept when this is necessary for the conduct of your research.

Where identifiable information is necessary, pseudonymisation should be carried out as soon as possible in the research process. Pseudonymised data must have appropriate measures in place to ensure their security. Please see **Keeping data safe and valid** for further guidance.

Pseudonymisation may introduce delays and increase risks of error. Where this risk poses a significant threat to research delivery, it must be managed. This may involve implementation of a standard operating procedure, training of staff and monitoring. If significant errors are identified, a review should be undertaken. Reviews should consider any lessons learnt and make changes to processes, in order to minimise the risk to data validity and security in the future. It's worth noting that even a simple pseudonymisation system can provide safeguards against accidental or mischievous release of confidential information without compromising data integrity.

In some clinical studies frequent reference by research and medical staff to current patient conditions is necessary. Continual pseudonymisation and re-identification of information in these circumstances can pose a significant obstacle to effective team work, and increase the risk of error which could affect patient care. The use of indirect identifiers (such as patient initials) when processing information is acceptable, when only a small number of research staff will have access to the information and consent to take part in the research is in place. In cases where datasets still contain indirect identifiers, this information should be subject to the same rigorous physical and information security arrangements as identifiable information.

Within research teams, only those who need to see or use identifiers should have access to them. The remainder of the team should have access to only pseudonymised data. The Principal Investigator should manage access to identifiable information, ensuring that only those who both need access and are competent to use it are given permission to do so.

Related links

1. Information Commissioner's Office Anonymisation Code of Practice **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**
2. UK Anonymisation Network decision-making framework **http://ukanon.net/ukan-resources/ukan-decision-making-framework/**

6. Data sharing and publishing

When sharing data, you should limit disclosure of any identifiable information and ensure that any disclosure complies with the law. Please see **Summary of relevant law** for more guidance.

Sharing data with others

Sharing data is common practice in research, and is actively encouraged to ensure that maximum use can be made of good quality data. The use of research data should be maximised to help address important research questions.

In most cases any data shared will be anonymised. 'Anonymised data' leaving the research team must have adequate controls in place to prevent (re)identification. This should include consideration of any other sources of information that the recipient may have access to, which could enable identification of participants when combined with the transferred information – for more please see **Anonymisation and Pseudonymisation**.

'Identifiable information' should usually only be shared with others if there is a legal avenue for disclosure, this is what research participants would expect, and the amount and sensitivity of the information is minimised. Participant expectations should be managed through the consent process, with adequate and open information about intended or planned sharing being made available at the outset. If you intend to share identifiable information about an individual research participant with other researchers then you should do so with explicit consent and it must be shared securely (e.g. with adequate encryption / information security). If collaborators do not need to see identifiable information, but can work just as effectively with anonymised data, no identifiers should be passed to them. In addition, collaborators may not require the entire dataset; therefore, only the data essential for the planned research should be transferred.

The Principal Investigator is accountable for ensuring that adequate precautions are put in place to enable responsible sharing of research data. They should work with their legal / contractual colleagues to ensure that adequate Data Transfer / Sharing Agreements are in place when sharing data with others. In such agreements, each party should set out what data are to be supplied, how they can be used and what will happen to these data when the research project is complete. This should include clauses that limit further disclosure of the information by recipients and ensure that recipients do not attempt to re-identify any individual participants from anonymised datasets.

Where data sharing requests are received, there should be a process in place to check both the authenticity of the researcher and their planned research. (This process may be reinforced with auditing, to ensure that any data shared are being used in line with any terms agreed).

The MRC has further guidance on open research data[1] and good practice principles for sharing individual level participant data[2] developed by the Methodology Hubs.

Sharing data outside of the European Union

Ideally any data shared outside of the European Union (EU) will be 'anonymised data' - see also **Anonymisation and Pseudonymisation**. Sending personal data out of the EU might include the use of cloud computing storage (i.e. where the cloud's servers are located outside the EU, e.g. in the US). If you intend to send 'personal data' outside the EU you need to consider the requirements of GDPR and the UK Data Protection Act 2018 - see International Transfers on the ICO website[3]. Before making decisions to send personal data out of the EU, Principal Investigators should discuss what they plan to do with their organisation's Data Protection Officer.

Publishing information in the public domain

There is an ethical imperative to publish the results of research (e.g. in scientific journals, at conferences etc.). The MRC champion Open Access publishing[4], which provides free and unlimited access to research results. When publishing in the public domain, it is usually preferable to publish only ‘anonymous data’ where there is no risk of identification. Please select **Anonymisation and Pseudonymisation** for further guidance.

Where it is not possible to publish anonymous / anonymised outcomes (for example where outcomes relate to very small populations such as one family or require publication of photographs of individuals with visibly recognisable conditions), research participants should be told this during the consent process. If ‘personal data’ about individuals is to be published, then the participant to whom this relates maintains the right to access their data. If you receive such a request from any participant please contact your local Data Protection Officer for advice.

In some cases (e.g. to support open science) individual participant level data may be published as stated in the Methodology Hubs guidance where very robust ‘anonymisation’ has taken place. However, in most cases, to enhance privacy the MRC supports managed access to such individual participant level data.

Related links

1. MRC Open research data: clinical trials and public health interventions **https://mrc.ukri.org/research/policies-and-guidance-for-researchers/open-research-data-clinical-trials-and-public-health-interventions/**
2. MRC Hubs for Trials Methodology Research, Good practice principles for sharing individual participant data from publicly funded clinical trials **http://www.methodologyhubs.mrc.ac.uk/files/7114/3682/3831/Datasharingguidance2015.pdf**
3. ICO GDPR guidance on International Transfers **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/**
4. RCUK Open Access policy **https://mrc.ukri.org/research/policies-and-guidance-for-researchers/open-access-policy/**

7. Accessing central sources of data

There may be circumstances when accessing existing central sources of data (e.g. from NHS Digital, the Office for National Statistics, Information Services Division etc.) will help you answer your research question or trace participants lost to follow up.

These organisations provide access to anonymous, anonymised or identifiable NHS and other central sources of data which are created by specialist staff using technical solutions such as indexing, data linkage etc. To find out how to access this data please see the MRC Regulatory Support Centre webpage[1] which lists a number of helpful resources.

If you are accessing confidential patient information without consent from NHS Digital (i.e. when you will be accessing confidential patient information from NHS Digital with Section 251 approval), patient opt outs will be applied and the dataset will be incomplete. For further information please see National data opt-out programme[2].

Where you have accessed central NHS data from NHS Digital and you intend to share these data with others, NHS Digital require you to do so under a third-party agreement.

Related links

1. MRC Regulatory Support Centre, How can I access health data? **https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/supporting-research-using-health-data/**
2. NHS Digital National data opt-out programme **https://digital.nhs.uk/services/national-data-opt-out-programme**

8. Keeping data safe and valid

The key to keeping data safe is having controls and measures in place which ensure the protection of research participants' privacy and prevention of any unintended or accidental disclosure. Please see **Summary of relevant law** for further guidance on the law in this area.

Keeping data safe

There are a number of controls and measures which organisations should put in place to keep data safe. These should focus on reducing the identifiability of data / minimising the risk of (re)identification and ensuring data security:

- Minimise use of identifiable information (see Principle 5, available from **Principles** in the menu)
- Limit access to identifiable information (see Principle 6, also in **Principles**)
- Security – Principal Investigators should ensure that identifiable information is secure (e.g. by working with relevant experts and to local information security policies).
- Contractual obligations - You should be aware of any implications of data transfer / sharing agreements pertinent to the information you handle. These agreements may stipulate that you comply with additional requirements.

Whenever practical and reliable you should hold either 'anonymous data', 'anonymised data' or 'pseudonymised data'. Please see **Anonymisation and pseudonymisation** for further guidance.

All information about people must be kept in line with local information security policies, to ensure compliance with the law and other pertinent requirements (e.g. Cabinet Office rules where relevant). To this end it is vital that you work with relevant experts within your organisation to ensure that appropriate measures are in place, before any information about people is collected. Particular care must be taken when:

- Disposing of old IT equipment that has been used to store 'identifiable information' for research (i.e. to ensure all identifiable information is removed before disposal).
- Managing off-site maintenance of IT equipment that has been used to store identifiable information.
- Using mobile technology to collect and physically move identifiable information from place to place. Mobile technology should only be used when this is justifiable and with adequate levels of encryption.

The role of the research team

Principal Investigators must ensure that all those handling information about people (including students, visitors, collaborators etc.) have the relevant expertise in information security and local / study specific procedures before they handle such information.

All staff involved in the collection, collation and handling of information about people should have received appropriate training or exhibit demonstrable expertise in local information security policies. Many organisations that provide you with research information (e.g. NHS Digital in England and Wales and the Information Services Division (ISD) in Scotland) will expect you to demonstrate what training you have received and your relevant expertise, before releasing data to you.

Before research starts, specific responsibilities should be agreed and assigned for the following:

- Overall management and control of research data
- Rapid response to breaches of security
- Management of software
- Maintenance of backup and disaster recovery
- Control and minimisation of duplicate files
- Control of access rights and changing these in response to staffing changes etc.
- Disposal or archiving of data or parts of these data collected at the end of the study – see also Archiving.

All staff should have secure access only to the systems that they need to conduct their part of the study. They should have a valid account and user name for their organisation's IT network, which must not be shared with others and/or access to restricted network folders where appropriate. Users should ensure that at log-off, documents recently used and containing identifiable information are cleared from applications on start up.

Ensuring data remains valid

Principal Investigators must work with relevant experts to ensure that the appropriate infrastructure is in place to effectively ensure the validity of their research data. Advantage should be taken of technological approaches to validity checking. These may include automatic flagging of errors at the time of data entry (e.g. birth dates outside likely time frames, unusual anthropomorphic or biological measures etc.).

Significant errors can occur when collating, anonymising / pseudonymising, linking and transcribing information, etc., which can pose a significant risk to the delivery of your research. Staff handling data may require:

- Standard processes to follow when conducting higher risk information handling procedures
- Simplification of processes to aid compliance;
- Training in protocol specific data handling procedures relevant to their role (in addition to training in local information security policies)
- Monitoring to ensure that any errors can be detected, corrected and processes put in place to further limit the risk to data validity. Monitoring should be risk informed, with an emphasis placed on those activities that are considered higher risk with respect to data validity.

9. Working without consent

There may be times when you wish to access existing datasets held by others either to address your research question or to trace participants lost to follow up.

For example:

- Identifying potential participants who have tumours that have or have not responded to a specific treatment, in order to invite these people to give consent to take part in your study
- Epidemiological study collecting health information about all those born in a defined geographical area during a defined period of time
- A study collecting information about asthma treatment from medical notes held by GP practices
- Re-contacting a cohort of previous study participants, but first wishing to check current address, whether alive or dead and health status prior to making contact
- You intend to use confidential information about people who are now dead, and who were not given the opportunity to consent to your study prior to their death

When you **do not** have consent to use confidential information for health and social care research you must still ensure identifiable information is handled in compliance with the law. Please select **Summary of Relevant Law** for further guidance on Accessing identifiable information without consent and the Common Law of Confidentiality, GDPR and the UK Data Protection Act 2018 also apply (e.g. you need to be lawful, fair and transparent).

Appropriateness of disclosure

Before applying for any approval to allow the disclosure of confidential information outside of an established duty of confidence without consent, you should consider the appropriateness of what you are proposing. You must only use 'identifiable information' for research if it is necessary, justified and unlikely to cause harm or distress.

You might consider applying the following tests to judge whether disclosure without consent is appropriate:

- If the proposed disclosure and the reasons for it became widely known, would a reasonable person of ordinary sensibilities see it as unacceptable? or
- Apply the narrower test; are there any grounds for supposing that, if consent could be sought effectively, reasonable people would be likely to refuse the use of their records?

Alternatives to disclosure of confidential information

If you don't have consent or an alternative legal basis to access confidential information:

- Is it possible to conduct your research without the research team accessing or using confidential information (i.e. by using 'anonymised data')?
- Is it possible to manage the study such that only the 'care team', or the organisation holding these data access confidential information?
- Is it possible to manage disclosure through the use of technology that enables datasets to be linked or for specific items to be searched for and data elements extracted without breaching confidentiality?

Limiting disclosure

You should both satisfy yourself and demonstrate within any application for approval that you will collect the minimum amount of information with the least degree of sensitivity. Therefore, ensuring that only the confidential information required to meet your study end points are disclosed.

You must also have processes in place to ensure that any 'identifiable information' disclosed to you is kept secure - see Keeping data safe and valid.

10. Archiving

Arrangements for data management, storage and longer-term archiving should be considered even before the study begins. It's important to consider the protection of research participants' privacy and the prevention of any unintended or accidental disclosure which may potentially arise from longer-term archiving.

Please see **Summary of relevant law** for further guidance on the Common Law of Confidentiality, GDPR and the UK Data Protection Act 2018. In terms of archiving, data protection law does allow research data to be kept for longer periods. Indeed researchers can keep data indefinitely, see ICO's GDPR guidance: How long can we keep personal data for archiving, research or statistical purposes?[1]

Potential research participants should be made aware of your plans to store their data after the study has ended (e.g. during the consent process or via a 'privacy notice'). This should include how long data will be kept, which organisation will be responsible for it, what measures will be taken to protect confidentiality, and whether there are any intentions to share data with others, etc.

For further guidance on making decisions about archiving please see the Retention framework for research data and records[2].

Related links

1. ICO GDPR guidance on storage limitation (relevant for research data) **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/#archiving**
2. MRC Regulatory Support Centre: Retention framework for research data and records **https://mrc.ukri.org/documents/pdf/retention-framework-for-research-data-and-records/**

Glossary

Anonymisation: The process of turning data into a form which does not identify individuals and where identification is not reasonably likely to take place. This allows for a much wider use of the information. For further guidance on Anonymisation please see the ICO Anonymisation code of practice[1].

Anonymised data: Is data that does not identify an individual directly and that is unlikely to allow any individual to be identified through its combination with other data. To ensure data is anonymised you must mitigate the risk of identification until it is no longer reasonably likely (e.g. by controlling the risk of (re)identification through the use of legal agreements etc.). Anonymised data can be achieved by following the ICO Anonymisation code of practice[1], or similar processing.

Anonymous data: Is data from which an individual cannot be identified. The term describes most aggregate data e.g. 200 hip replacements were performed in a specific hospital in 2016. It may include some individual participant level data where there is no risk of (re)identification e.g. a 62-year-old with high cholesterol. Anonymous data are suitable for release into the public domain.

Care team: The health and/or social care professionals and staff that directly provide or support care to an individual. The care team can consist of registered and regulated professionals (such as physiotherapists, nurses, midwives, occupational therapists and others on regulated professional registers) or un-registered and non-regulated staff (such as healthcare support workers, GP Receptionists or hospital porters). Researchers with a clinical role can often be part of the care team. The key to determining whether someone is part of the care team or not, is if they directly provide or support the care of a patient. For more details please see Sections 3.6 and 3.7 of Information to share or not to share: The Information Governance Review[2].

Confidential patient information: Is defined in section 251 of the NHS Act 2006:
'**Patient information**' means:
(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and
(b) information (however recorded) which is to any extent derived, directly or indirectly, from such information,
whether or not the identity of the individual in question is ascertainable from the information

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.

COPI regs: The Health Service (Control of Patient Information Regulations) 2002 (S.I. 2002/1438), as amended by Section 117 of the Care Act 2014, make provisions for 'confidential patient information' in England and Wales to be processed without consent for medical purposes, including medical research, where it would not be reasonably practicable to achieve that purpose otherwise, having regard to the cost of and the technology available for achieving that purpose.

Data Controller: Any person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any 'personal data' are, or are to be, processed. This may be an individual or, more likely, an organisation registered with the Information Commissioner's Office.

Data Processor: Any organisation / person (other than an employee of the Data Controller) who processes 'personal data' on behalf of the Data Controller. The Data Processor and Data Controller usually formalise processing responsibilities within a contractual agreement.

Data Subject: Any natural person (i.e. living individual) whose 'personal data' is held by a Data Controller.

Disclosure: The release of information to a third party.

Disclosure is often thought of as something to be avoided (e.g. accidental or unintentional disclosures caused by lost memory sticks, confidential papers left in a public place or a determined intruder such as a computer hacker). However, there are circumstances when the disclosure of identifiable information to a third party is entirely appropriate and in compliance with the law.

Duty of confidence: You owe a duty of confidence when you know information about an identifiable individual and they have a reasonable expectation of privacy with respect to that information (e.g. patient and doctor). Confidential information should only be revealed to those that the individual might reasonably expect in the circumstances (e.g. with consent or with an alternative legal basis).

Identifiable information: Information from which an individual can be directly identified or can be identified by combining with other information that is reasonably likely to be available. When considering whether information is identifiable or not it is important to consider both the content of the information and the context in which it is viewed. Even when subject to a process of 'anonymisation' some datasets may contain potential identifiers (e.g. unusual birth dates, photographs of specific conditions, research participants with rare conditions or from small communities, etc.). Care must be taken with some types of information (e.g. parts of postcode, year of birth etc.) which when viewed alone may not be identifying, but through combination become identifying.

Identifiable information may be subject to a 'duty of confidence'.

Identifiable information may also be 'personal data' and/or 'sensitive personal data'.

Information Commissioner's Office: The Information Commissioner's Office (ICO) is the UK regulator responsible for providing advice and guidance to ensure compliance with GDPR. The ICO are also responsible for ensuring compliance with the Freedom of Information Act (2000) in England, Wales and Northern Ireland. Scotland has its own Information Commissioner who regulates the Freedom for Information (Scotland) Act (for further details please see the Scottish Information Commissioner website[3]).

Legitimate relationship: Is defined in Information to share or not to share: The Information Governance Review[2] as the legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care.

Personal data: Any information relating to natural persons (i.e. living individuals) who:

- can be identified or who are identifiable from the information in question; or
- who can be indirectly identified from that information in combination with other information.

For more information please see ICO's GDPR guidance – What is personal data?[4]

Privacy Notice / privacy information: Information provided by the 'Data Controller', which communicates how the organisation collects, uses and protects 'personal data'. Although often referred to as a 'privacy notice', privacy information should not be delivered in a single notice. Rather it should be provided in more than one way and through a variety of media (e.g. verbally, in leaflets, posters, on websites, etc.). Privacy information provided by research active hospitals, general practices and other health care organisations should include details of how data are used for research. Patients should have a degree of control and choice over how their data will be used (e.g. if they object to their data being used in research, they should have the opportunity to stop this). Effective privacy information ensures 'data subjects' are informed, and meets the requirement for 'transparency'. Please see the ICO's GDPR guidance: Right to be informed[5].

Processing: The processing of 'personal data' includes obtaining, recording, holding or carrying out any operation on the data. For details of who can carry out processing of personal data, please also see 'Data Controller' and 'Data Processor'.

Pseudonymisation: The process of creating 'pseudonymised data' with the use of a pseudonym (i.e. a decryption key or cipher only available to a limited number of people in the research team). For further guidance on pseudonymisation please see the ICO's Anonymisation code of practice[1].

Pseudonymised data: Is 'personal data' that has been processed in such a way that it can no longer be attributed to a specific individual without the use of additional information (e.g. a decryption key or cipher to which only a limited number of the research team have access). This is used to limit the risk of inappropriate disclosure.

Pseudonymised data are still regarded as 'personal data' because the same organisation has access to the dataset in its entirety (i.e. the pseudonymised data and the decryption key or cipher). Personal data should be handled in accordance with GDPR. For further guidance on pseudonymised data please see the ICO's Anonymisation code of practice[1].

Special categories of personal data: Are defined in GDPR to mean the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The processing of genetic data and/or 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.

Related links

1. Information Commissioner's Office (ICO) Anonymisation: managing data protection risk code of practice **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**
2. Dame Fiona Caldicott, Information: To share or not to share? The Information Governance Review, March 2013 **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf**
3. Scottish Information Commissioner website **http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx**
4. ICO GDPR guidance - What is personal data? **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/**
5. ICO GDPR guidance on the right to be informed **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/**

Acknowledgments

These principles and guidelines were developed in 2016/17 by the MRC Regulatory Support Centre and reviewed by the MRC Ethics, Regulation & Public Involvement Committee (membership is detailed below). We are very grateful to all members of ERPIC, and to all who contributed to the guidelines. Although we would like to extend particular thanks to Dr Mark Taylor who has been instrumental in the development of this guidance.

Members of MRC Ethics, Regulation & Public Involvement Committee (ERPIC) (in alphabetical order):

Dr Louise Bowman	Clinical Trial Service Unit, University of Oxford
Ms Sally Crowe	Crowe Associates/Chair of James Lind Alliance
Dr Sarah Edwards	Centre for Philosophy, Justice and Health, University College London
Dr Michael Emerson	National Heart & Lung Institute, Imperial College
Dr Jonathan Hewitt	Cardiff University
Professor Emily Jackson	London School of Economics
Dr Neil Manson	Lancaster University
Baroness Onora O'Neill	Chair of ERPIC and member of the MRC Council
Ms Vivienne Parry OBE	Writer and broadcaster specialising in science and medicine
Dr Mark Taylor	University of Sheffield

MRC Staff (in alphabetical order):

Ms Heather Coupar	Regulatory Manager, MRC Regulatory Support Centre
Dr Sarah Dickson	Head of MRC Regulatory Support Centre
Dr Jon Fistein	Former Head, Clinical Ethics and Data, MRC
Dr Rachel Knowles	Clinical and Population Research Specialist, MRC
Dr Declan Mulkeen	Chief of Strategy, MRC
Dr Frances Rawle	Head of Corporate Governance and Policy, MRC
Mrs Rachel Robertson	Resource Development Manager, MRC Regulatory Support Centre
Dr Rachel Smith	Head of Training and Partnerships, MRC Regulatory Support Centre