Chapter 4: Accountability and governance

Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance

March 2022

ico.
Information Commissioner's Office

Contents

What accountability and governance measures are needed for anonymisation? 2

What governance approach should we take? 3

Who should be responsible for our anonymisation process? 4

Should we do a Data Protection Impact Assessment? 4

Are we clear about why we want to anonymise personal data? 5

How should we work with other organisations, where necessary? 7

What type of disclosure is it? 8

How should we identify potentially difficult cases? 10

How should we ensure transparency? 11

How should we ensure appropriate staff training? 12

How should we keep updated with legal and technical developments? 13

How should we mitigate re-identification risk due to a security incident? 14

What other legal considerations apply? 15

What accountability and governance measures are needed for anonymisation?

At a glance

- When producing and disclosing anonymous information, you should take a comprehensive approach to governance.
- Being clear about processes, responsibilities and oversight makes compliance easier.
- You should use a DPIA to help you structure and document your decision-making processes around anonymisation and identify risks to rights and freedoms and mitigation strategies in a structured way.
- You should be clear about how and why you intend to anonymise.
- You should work with other organisations likely to be processing, and possibly disclosing, other information that could impact the effectiveness of your anonymisation.
- You should consider how different forms of anonymous information can pose different identifiability risks and choose an appropriate release model to mitigate them.
- You should plan for cases where it may be difficult to assess identifiability risk and implement appropriate risk mitigation measures.
- Demonstrating transparency when processing anonymous information promotes public trust and mitigates the risk of any potential negative public opinion of the processing.
- You should ensure decision-makers have a clear understanding of the latest technological and legal developments and best practices to ensure effective anonymisation.
- You should consider any other legal considerations that may be relevant to your anonymisation processes and decision-making.

In detail

- What governance structure should we take?
- Who should be responsible for our anonymisation process?
- Should we do a Data Protection Impact Assessment (DPIA)?
- Are we clear about why we want to anonymise personal data?
- How should we work with other organisations, where necessary?
- What type of disclosure is it?
- How should we identify potentially difficult cases?
- How should we ensure transparency?

- How should we ensure appropriate staff training?
- How should we keep updated with legal and technical developments?
- How should we mitigate re-identification risk due to a security incident?
- What other legal considerations apply?

What governance approach should we take?

If you anonymise personal data, your governance approach needs to address the practical issues surrounding the production and any disclosure of this information.

Establishing an appropriate governance structure can improve your data management, record-keeping and disclosures of data. In addition, it is useful if you need to demonstrate compliance to the ICO.

Enforcement action, including the imposition of monetary penalties, is less likely if you can demonstrate that you:

- made a serious effort to comply with data protection law; and
- had a genuine reason to believe that the information was not personal data (ie by showing that identifiability risk was sufficiently remote).

A governance structure should cover the following areas:

- **How will you plan for anonymisation?**
  - Who is responsible for your anonymisation process?
- **How will you identify and mitigate anonymisation risks?**
  - Have you completed your data protection impact assessment (DPIA)?
  - Why do you intend to anonymise personal data?
  - How will you work with other organisations, where necessary?
  - Will you use a trusted third party (TTP)?
  - What are the relevant considerations for the type of disclosure, including limited access safeguards?
  - How will you identify and manage potentially difficult cases?
  - How you will ensure transparency?
- **How will you ensure anonymisation remains effective?**
  - How will you keep updated with relevant changes to the legal framework (including guidance and case law) and technological developments?
  - How you will ensure appropriate staff training?

- How will you approach re-identification testing?

- **How will you consider other relevant legislation?**
  - Are there any other legal considerations apply?

You should document the key decisions you make and the rationale for them as part of your accountability obligations.

Who should be responsible for our anonymisation process?

Make sure that someone of sufficient seniority oversees your anonymisation process and associated decision-making. This may be a single individual or a group of authorised persons, depending on your circumstances. They should work closely with your DPO to seek their advice and guidance (if you are required to have one). They should have an appropriate understanding of:

- the circumstances both of your process and any intended disclosure; and
- relevant technical and legal considerations.

Data protection law does not specify who this person may be or what their formal role is. The important point is that they must have appropriate authority.

For some organisations, adopting a Senior Information Risk Owner (SIRO) approach can be particularly useful. In this context, the SIRO:

- takes responsibility for key decisions and informs your general approach to anonymisation;
- consults with your DPO to obtain their independent expert advice;
- coordinates a corporate approach to anonymisation, drawing on relevant expertise from within and outside your organisation; and
- helps you decide on suitable forms of disclosure (ie publication or limited access).

Should we do a Data Protection Impact Assessment?

A DPIA enables you to assess risks to rights and freedoms in a structured way. It is also a useful tool to help you structure and document your decision-making processes. It is likely to form a key element of your overall governance structure for processing personal data. It can also have relevance in the context of anonymisation.

For example, a DPIA can help you assess the impact of anonymisation on your overall risk. It can assist you to decide:

- whether to anonymise in the first place;

- whether using anonymisation techniques reduces any risk to rights and freedoms (eg because the data no longer identifies individuals);
- what risks may present if the anonymisation is ineffective, and the steps you intend to take to mitigate them; and
- the particular techniques, measures, safeguards and testing approaches of your anonymisation process.

You must do a DPIA for processing that is **likely to result in a high risk** to individuals. We also require you to do a DPIA if you plan to:

- use innovative technology; or
- match data or combine datasets from different sources.

Rendering personal data as anonymous information may require using innovative technologies. For example, the use of PETs to pool datasets from various sources and applying anonymisation techniques, such as differential privacy, to generate anonymous information from them. In these cases, you need to complete a DPIA. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project when generating anonymous information from personal data.

You can easily apply the approach in our guidance on DPIAs to many anonymisation scenarios.

Relevant provisions in the legislation

See UK GDPR Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95

See DPA 2018 section 207 (external link)

Further reading – ICO guidance

See the section of this guidance on 'How do we ensure effective anonymisation?'' for more information on assessing identifiability risk.

For more information, see our detailed guidance on DPIAs in the Guide to the UK GDPR.

We have also produced a suggested template for a DPIA (please note this link will download a Word file).

Are we clear about why we want to anonymise personal data?

The process of anonymising personal data involves an operation, or set of operations, performed on that data. It is therefore "processing" for the purposes of data protection law. You should be clear about how you

anonymise personal data and why you intend to do so in your governance approach.

In general, the act of anonymising the personal data you hold must be fair and lawful. After all, the intended result of your anonymisation process is a dataset that does not include information about identifiable individuals.

Anonymisation therefore provides significant benefits from a data protection and privacy perspective, both for you and the individuals whose personal data you process.

For example, the processing of anonymous information poses significantly lower risks to the rights and freedoms of individuals. If individuals are not identifiable then the dataset may not allow you to take decisions about them or treat them differently. The impact on individuals is likely to be minimised.

When you anonymise you need to define your purpose and the detail the technical and organisational measures to achieve it. A key aspect of your considerations should be clarifying the context and purposes for anonymising.

This is because anonymisation may be:

- an aspect of your overall processing activities; or
- the overall purpose of your processing.

Whether this is the case depends on your circumstances, so it is important to be clear on when you intend to anonymise and why.

Anonymisation as part of your processing activities

Where anonymisation does form part of your overall processing activities, it can be a way to comply with the data protection principles. For example, to comply with the principles of data minimisation and storage limitation, you have to:

- collect only the personal data you need for your purpose; and
- keep it in a form that identifies individuals only for the time you need to achieve that purpose.

Once you achieve your purpose, you can either erase or anonymise the personal data, depending on your circumstances.

In these situations, anonymisation may simply be something that you do as part of the processing and as a way of complying with the law. As long as your anonymisation is effective, subsequent use of the anonymous information is not something data protection law applies to.

In many cases, processing of personal data to anonymise it is likely to be compatible with the original purpose(s) you collected it for, unless:

- there is a reasonable expectation from an individual that you will retain the data in identifiable form; or
- when you collected it, you told them you intended to keep it in that form.

When making your assessment, you should consider if the result of your anonymisation process is a dataset in which individuals cannot be identified, or are no longer identifiable? This is important when you consider the possible consequences of the anonymisation on individuals.

Anonymisation as part of your purpose

Anonymisation may itself be a way in which you achieve the purpose for which you originally collect personal data.

For example, if your purpose is to generate aggregate statistical information about how individuals engage with your service, you may need to collect information about what each one does first.

This is likely to be personal data, as it relates to actions and behaviours that specific individuals take. You should therefore ensure you are clear with individuals that this is why you want to collect their data.

However, collecting this data is a first step towards achieving your purpose - creating the aggregate information. You can then apply anonymisation techniques that create an aggregate dataset. This allows you to identify trends and behaviours in a generalised manner.

How should we work with other organisations, where necessary?

If you are planning to disclose any anonymous information you should work with other organisations likely to be processing, and possibly disclosing, other information that could impact the effectiveness of your anonymisation. For example, organisations disclosing information which might allow the individual to be identified that the anonymised information relates to.

A joined-up approach with other organisations in your sector, or those doing similar work, allows you to assess the risks collectively and agree mitigations, where appropriate.

For example, if public authority A is planning to disclose anonymous information about health, it may be helpful for it to know that public authority B is also planning an anonymised disclosure about welfare at the same time, with both using similar geographical units. Both authorities can then assess the risks jointly.

Further reading – ICO guidance

Using a Trusted third party (TTP) is one way of working with other organisations in a trusted environment.

We will be exploring various TTP models, use cases and compliance in later sections of this guidance.

We will update this box once the guidance is published.

What type of disclosure is it?

Different forms of anonymous information can pose different identifiability risks. In general:

- open release can be riskier than limited access; and
- limited access allows the disclosure of "richer" data but its success relies on robust governance arrangements.

You should draw a distinction between publishing anonymous information to the world at large and limited access disclosures. For example:

- publication to the world at large (eg under open data or FOIA) means there is no restriction on the further disclosure or use of that data and no guarantee it will be kept secure; and
- limited access (eg within a closed community of researchers) means it is possible to restrict the further disclosure or use of the data, and provide better guarantees about its security.

The more detailed the information is, the stronger the argument for limited access over general disclosure. The more aggregated and non-linkable, the more possible it is to publish but the more robust your identifiability risk assessment needs to be.

Open data relies on public availability of information. Additionally, you cannot restrict information released under the Freedom Information Act (FOIA) to a particular person or group.

For activities such as research, systems testing or planning, limited access may be more appropriate. For example, releasing data among a closed group with a finite number of researchers or institutions involved. You should prohibit further disclosure by contractual controls backed up by robust technical and organisational measures. This enables identifiability risk to be more controllable while also allowing you to disclosure more data without leading to the same risks that arise with open release.

What limited access safeguards should we consider?

Limited access is particularly appropriate for handling anonymous information derived from sensitive source material, depending on the circumstances. There can still be risks with limited access. For example, further disclosure outside the group or for purposes beyond what has been agreed. However, you may mitigate these risks by ensuring that you disclose anonymous information in a closed community with clear, established rules (including around data minimisation).

If you are responsible for disclosing data on a limited access basis, you should put robust safeguards in place, before making the anonymous information available to others. These should include (but are not necessarily limited to):

- purpose limitation – the recipient(s) can only use the anonymous information for an agreed purpose or set of purposes;
- training of recipients' staff who will have access to the data (eg on security and data minimisation principles);
- security checks for those who will access the data;
- controls over the ability to bring other data into the environment to manage identifiability risks arising from linkage or association;
- limiting data use to a particular project or set of projects;
- restricting disclosure of the data outside the limited access environment;
- prohibiting attempts at re-identification;
- ensuring appropriate measures are in place to destroy any accidentally re-identified personal data;
- implementing appropriate technical and organisational security measures, including confidentiality agreements for those who will access the data (including your staff);
- restricting access to the data (eg by applying appropriate encryption techniques and access control policies);
- limiting the number of copies of the data to what is necessary for the purposes of the disclosure;
- arranging for the destruction or return of the data and confirmation of completion thereof once the project is complete; and
- imposing appropriate penalties if any recipient breaches the conditions placed on them (eg as part of contractual requirements).

You need to conduct your own risk assessment using your normal data security risk assessment processes to decide which apply. However, you should also co-ordinate with the other parties involved in the project to establish if you should include additional security measures.

What about publication under licence?

Once data is published under a open licence such as the Open Government Licence (OGL), Creative Commons Licence or Open Data Commons, it may be impossible to protect it from further use or disclosure, or to keep it secure.

Open data licencing models are clear that while anonymous information is within scope of their conditions, those using the information are not permitted to do so in a way that enables re-identification to take place. However, in practice this may be difficult or impossible to enforce.

Therefore your anonymisation processes and identifiability risk assessments need to take this into account.

Other data licencing models include:

- 'Safeguarded' access intended for data with some risk of re-identification. However, there are strong technical and organisational measures in place such that it is regarded as non-personal data under data protection law.
- 'Controlled' or secure access data that has been subject to data minimisation techniques (eg pseudonymisation), but remains identifiable and is therefore still personal data.

Further reading

The UK Data Service provides further guidance on the terms of use for various public-sector licencing structures.

How should we identify potentially difficult cases?

Your governance approach should cater for cases where it is difficult to assess identifiability risk, or where that risk may be significant. This may mean that effective anonymisation is difficult to achieve in practice. Where anonymisation is ineffective you continue to process personal data and remain responsible for complying with data protection obligations.

Anonymisation can be ineffective due to several factors, for example:

- You can only meet your objectives using personal data; or
- technological developments such as the emergence of new attacks and increased computational power mean that the anonymisation techniques you applied are no longer effective.

You should consider whether alternative state-of-the-art techniques are available to ensure that the data is effectively anonymised and if there are technical and organisational measures to mitigate the risk of re-identification.

Your governance approach should also cater for other risks relating to the use of anonymous information. For example, you should:

- only use anonymous information in ways individuals would reasonably expect;
- consider whether individuals would reasonably expect you to retain the data in identifiable form; and
- assess whether rendering personal data as anonymous information would affect related individuals and how any adverse impact can be justified.

The level of risk depends on the nature and context of the processing. For example, special category personal data such as an individual's health status or ethnicity which is subsequently anonymised is likely to carry more risk.

As part of your DPIA you need to consider the risk of:

- using anonymous information for further purposes which may to lead to detrimental effects on an individual (eg discrimination or financial loss); and
- using anonymous information with poor analytical value, which may lead to detrimental effects on an individual. For example, anonymous information related to demographic characteristics which introduce bias. In this case, you should consider whether it is possible to adjust the level of accuracy while ensuring it remains anonymous.

It is good practice to have these procedures to identify difficult cases and to document your decision-making.

How should we ensure transparency?

As processing anonymous information theoretically has no direct effect on any individual, it may seem unclear why individuals should know about it. Additionally, it may not be necessary, and in many cases will be impossible, to contact individuals. Demonstrating transparency when processing anonymous information promotes public trust and mitigates the risk of any potential negative public opinion of the processing.

However, individuals have the right to know how and why you are processing their data. Your organisation's privacy policy should explain your approach to anonymisation as clearly as possible, including any consequences it may have. The policy should be clear and easily accessible to individuals.

In particular, you should:

- explain why you anonymise individuals' personal data;
- describe the techniques that you use to do this (in general terms);

- say what safeguards are in place to minimise the risk that may be associated with the production of anonymous information. In particular, you should explain whether you intend to make the anonymous information publicly available or only disclose it to a limited number of recipients;
- be open with the public about any risks of the anonymisation you are carrying out, and the possible consequences of this. You should give them the opportunity to submit queries or comments about this; and
- describe publicly your reasoning for publishing anonymous information and explain how you did the "weighing-up", what factors you took or did not take into account and why, and how you looked at identification 'in the round'.

This type of transparency should improve trust as well as lead to improvements in your decisions through exposure to public scrutiny and comment.

Whilst it is good practice to be as transparent as possible, you should not disclose data that would make re-identification more likely. However, you should still ensure that you are open and transparent about your decision-making to mitigate the risk of generating public distrust and suspicion.

You should also consider whether you can publish any DPIAs or relevant reports about your anonymisation. This does not require you to publish the entire document. You can remove certain information if needed, or publish a summary.

You should also review the consequences of your anonymisation programme, particularly through analysing any feedback. This should be an ongoing activity. For example, technological developments may impact the effectiveness of your techniques and the outcome of any assessment of identifiability risk over a period of time.

It is important for you to be able to analyse and deal with any complaints or queries you receive from individuals.

How should we ensure appropriate staff training?

It is important that your members of staff who are involved in decisions about creating and disclosing anonymous information have a clear understanding of:

- the anonymisation techniques you use;
- any risks involved; and
- how to mitigate these risks.

In particular, individual staff members should understand their specific roles in ensuring anonymisation is done safely.

You should devise a training plan that maps out the appropriate level of training needed and that professional development is taking place to ensure staff remain suitably competent. As part of your plan you should consider training on:

- data protection, information governance, and information security; and
- the application of state-of-the-art anonymisation tools and techniques.

Having an effective training plan in place can mitigate the risk of mistakes that might compromise the effectiveness of the anonymisation. It also ensures that only people with the right motivation and skills perform anonymisation and helps to build and maintain public trust and confidence.

How should we keep updated with legal and technical developments?

If you are involved in anonymising data, it is important to keep up-to-date with any new guidance or case law that clarifies the legal framework surrounding anonymisation.

You should also ensure you keep up-to-date with new techniques that are available, including for:

- anonymising data; and
- identifying intruders that seek to unmask individuals within a dataset.

It is good practice to maintain effective knowledge management about these issues. This will help you to keep your decision-making and anonymisation processes up-to-date and reflect the state of the art. This does not necessarily mean you need to have a "formal" knowledge management process in place. Although, depending on your organisation this may be part of your internal structure already.

Further reading – ICO guidance

As well as the good practice laid out in this guidance, you should refer to other relevant publications and online resources. Some examples include:

- Technical publications from recognised technical bodies, for example ENISA and NIST
- Appropriate technology standards from ISO, IEEE, and IETF
- Peer-reviewed academic journals focusing on state-of-the-art technologies, eg Differential Privacy
- Peer-reviewed journals on practical data protection compliance, eg PDP Privacy & Data Protection

- Publications from relevant public-sector organisations, eg ONS intruder testing

Some useful resources for UK and EU case law relevant to anonymisation:

- CURIA - Transcripts of case law from the Court of Justice of the European Union and General Court of the European Union.
- Administrative appeals tribunal decisions
- British and Irish Legal Information Institute

We will be publishing further guidance on interpreting UK case law around anonymisation in the final version of the guidance.

How should we mitigate re-identification risk due to a security incident?

If a security incident leads to re-identification of an individual from data you treated as anonymous information prior to the incident, we would not consider this as a personal data breach at the time. This is providing you can demonstrate your decision-making to justify that the data was effectively anonymised. For example, if you followed the good practice in this chapter and documented how you used it to mitigate risks to individuals.

A re-identification incident may lead to the end of the anonymisation process or to its modification. For example, by using more rigorous anonymisation techniques or disclosure controls. Your governance procedures should address what you will do if you are concerned that the risk of re-identification has increased. For example, due to:

- technological developments (eg emergence of new re-identification attacks or stronger anonymisation techniques); or
- increased availability of additional information that when linked to the anonymised data may facilitate re-identification.

Applying state-of-the-art anonymisation techniques and adapting your approach in line with technological developments can help to minimise the risk of a re-identification incident occurring. For example, you should consider introducing some or all of the following measures to reduce the risk to a remote level:

- use a more rigorous state-of-the-art anonymisation technique;
- adjust the parameters of the anonymisation technique for increased privacy, (eg further generalisation or noise addition, if possible);
- implement stronger technical and organisational measures such as limited access safeguards and environmental controls; and
- ensure that re-identification testing considers state-of-the-art attacks.

In addition, you should consider applying technical measures such as encryption of the anonymous information. In the event of re-identification, this would render the data unintelligible to any person who is not authorised to access it.

What other legal considerations apply?

Other legal considerations may be relevant to your anonymisation processes and decision-making, depending on the nature of your organisation. In particular, public authorities often have additional legal obligations to consider.

How do freedom of information law and data protection law intersect?

The Freedom of Information Act 2000 (FOIA) covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002. Section 40 of FOIA includes a test for deciding whether you can disclose personal data to the world at large. This is dependent on whether disclosure to a member of the public would breach the data protection principles.

This means that if you are a public authority, you have to assess whether releasing apparently anonymous information to a member of the public would breach these principles. This ensures that you take into account the additional information that a particular member of the public might have. If they could combine the data to produce information that relates to and identifies a particular individual then this would become personal data.

Further reading – ICO guidance

Our chapter on 'identifiability' (How does the type of data release matter?) provides further guidance on disclosing anonymous information to the world at large.

The test in FOIA can be particularly difficult to apply in practice because different members of the public may have different degrees of access to the 'other information' needed for re-identification. A motivated intruder test can go some way towards addressing this problem.

In these cases, you should to try to look at identifiability 'in the round'. This means that you should assess whether any organisation or member of the public could identify any individual from the data you are releasing. This could be either from the disclosed data itself of from that data in combination with other available information.

The risk involved varies according to the local data environment and particularly who has access to information. This means that anonymised data disclosed within a secure local environment (eg when disclosed to a particular research organisation) could remain effectively anonymised even if it were published. The likelihood of re-identification would mean that the anonymised data would become personal data.

You may want to disclose data that is not personal data. Clearly, data protection law does not prevent this as non-personal data is out of scope. However, the fact that the data is not personal data does not mean you can always disclose it.

In the case of public authorities receiving a FOI request, another exemption may allow you to withhold the information. For example, FOIA's section 38 health and safety exemption could be relevant. The same considerations apply about disclosure under the Freedom of Information (Scotland) Act 2002.

There may still be reasons for withholding this data. Disclosing certain data could still present a risk to individuals, even if they cannot be identified from it. For example, a risk may arise if an educated guess leads to the misidentification of an individual. Available data plus individual knowledge might lead someone to believe that an innocent person was responsible for a particular crime. The reason for withholding anonymous information in these circumstances would be to protect the health and safety of the individual rather than to protect their data protection rights in the data.

The definition of personal data should not be extended to cover scenarios that involve information that does not relate to an identified or identifiable individual.

Further reading – ICO guidance

Read our Guide to FOI for more information.

Our chapter on 'identifiability' provides further guidance on how to assess what knowledge a motivated intruder may possess.

The Environmental Information Regulations 2004 (EIR) provide public access to environmental information held by public authorities. When you receive a request for information, you should also consider whether the information is the personal data of the requester or anonymous information. Read our Guide to EIR for more information.

How do human rights law and data protection law intersect?

It goes beyond the scope of this guidance to provide exhaustive guidance on the Human Rights Act (HRA). However, public authorities and private sector organisations must comply with the HRA, in so far as you carry out functions of a public nature.

Organisations subject to the HRA must not act in a way that is incompatible with rights under the European Convention on Human Rights. This includes Article 8 – the right to respect for private and family life. However, this is not an absolute right. Public authorities are permitted to interfere with it where it is necessary, lawful and proportionate to do so.

The Article 8 right often overlaps with the protections data protection law provides. If a disclosure is compliant with data protection law, it is likely to be compliant with the HRA. Remember that data protection rights apply only in relation to personal data and are not available where information has been anonymised so that is no longer personal data.

However, the Article 8 right is not limited to situations involving processing personal data. This means that some disclosures of information that do not engage data protection law could still engage the broader provision in the HRA. For example, information about people who have passed away might not be personal data but its disclosure may well breach the privacy rights of the family.

It is advisable to seek specialist advice if you believe a proposed disclosure has novel or potentially contentious Article 8 implications.

What other statutory prohibitions are relevant?

Other statutory prohibitions may apply to the disclosure of information, with different tests and considerations to the UK GDPR. For example, there are relatively strict limitations on the purposes for which certain government departments are allowed to produce and disclose even anonymised data. A breach of a statutory prohibition would engage FOIA's section 44 exemption.

What are the requirements for ensuring statistical confidentiality?

Producers of Official and National Statistics must observe the Code of Practice for Official Statistics, and the related National Statistician's guidance on confidentiality.

What are the differences between the common law of confidentiality and UK GDPR in terms of identifiability?

The common law duty of confidentiality (CLDC) governs sharing information that is obtained in circumstances where it is reasonable for a person confiding the personal information to expect that it will be held in confidence by the recipient. The legal duties of confidentiality apply independently of data protection law and can also apply to non-personal data. Data protection law can apply even where there is no duty of confidentiality, or a public interest ground permitting the disclosure of confidential data.

It is outside the scope of the ICO's functions and powers to provide specific guidance on the CLDC within the context of relevant legislation governing its processing. However, you should note that the CLDC extends beyond death,

and is therefore distinct from the definition of "personal data" under data protection law, which only applies to living individuals.

Data that has been obtained or generated by a medical professional who owes a duty of confidence is referred to as "confidential patient information"(CPI). However, CDLC can also apply in a very wide range of circumstances beyond the medical context. If the disclosure of CPI for medical research purposes is in the public interest and the data has undergone pseudonymisation, it is then out of scope of the CDLC, but is still regarded as personal data under data protection law.

Further reading outside this guidance

Confidential patient information is a legal term defined in section 251 (11) of the National Health Service Act 2006.

Further information on the CLCD can be found at the following links:

- Section of the General Medical Council's 'Ethics for Doctors' guidance on confidentiality (external link)
- NHS Code of Practice on confidentiality (external link)
- The Health Research Authority's guidance on 'Why is confidential patient information used?' (external link)