Health Data in Practice lecture series

Ethical and legal considerations in using patient data for research

Carol Dezateux

10th November 2020

Institute of Population Health Sciences

wellcome

Queen Mary University of London
Barts and The London

Learning Objectives

At the end of this lecture you will be able to

Understand

- DPA 2018, GDPR and the common law duty of confidence
- consent in research and confidentiality and the national patient opt-out
- The meaning of data protection in the context of the Data Protection Act 2018
- The seven key principles of the General Data Protection Regulation

Define:

- personal data (including special categories of data)
- anonymised and pseudonymised data
- data processors and data controllers

Describe

- the lawful basis for data processing to hold and use personal data to support research
- individual rights

Which are the main applicable laws to use of confidential information and personal data?

- The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998.
- The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data.
- Both came into effect on 25 May 2018
- The DPA sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions.
- The DPA and GDPR are laws enacted by statute.
- The common law duty of confidence is a common law and is also applicable when using confidential information

Consent in research

- Informed, voluntary and fair consent is the cornerstone of ethical research involving people.
- It is a mechanism to ensure the rights of individual participants can be respected and they can make an informed choice to participate, to not participate or to change their mind about participation.
- The common law is not overruled by statute law ie law written down in Acts, Regulations, etc. and passed by Parliament
- However consent is not likely to be the lawful basis by which research organisations hold and use personal data for research.
- Organisations must be fair and transparent with research participants about their uses of personal data
- This can be achieved through participant information and organisational notices which are required to be concise, transparent and intelligible.

Common law duty of confidence

- The law around information about people is complicated in the UK.
- We must also comply with the common law
- Common law dictates with whom confidential information can be shared.
- The common law demands that confidential information is managed in line with reasonable expectations **(no surprises).**
- Expectations can be managed by consent (implicit or explicit).
- The common law does allow disclosure even when this might not be reasonably expected, if disclosure is in the public interest, or another legal avenue is established (e.g. with Section 251 approval).
- The common law is not overruled by statute law i.e. law written down in Acts, Regulations, etc. and passed by Parliament
- The common law duty of confidence is not affected by implementation of GDPR or the Data Protection Act 2018

Information is considered confidential in law if

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

Can confidential information be disclosed without consent?

- When an individual entrusts a research team, or a clinical care team, with confidential information, the team must handle this information in line with 'reasonable expectations'.
- Confidential information should only normally be shared when there would be '**no surprises'** for the individuals concerned
- Important to limit sharing of confidential information
  - *Can it be anonymised?*
  - *Is there a public interest in disclosing confidential information eg crime, mental health concern?*
- In the UK there are legal avenues that allow the disclosure of confidential information to support medical research, even when this is not in line with 'reasonable expectations' (i.e. without consent) - for example, section 251 of Health and Social Care Act
- Approval under S251 doesn't affect an organisations legal obligations under GDPR and the Data Protection Act for the personal data they hold

National patient opt-out programme and the common law

- The national opt-out (in England only) developed by the National Data Guardian applies to the disclosure of confidential patient information under the common law duty of confidence, and not through data protection
- It gives patients an opportunity to opt out of specific non-care related uses of confidential patient information (anonymised information is not subject to opt-out)
- This preference is recorded and applied across the health and social care system
- Opt-outs do not apply where consent for disclosure for a research project is in place
- Opt-outs are normally respected under s251 unless there are strong scientific grounds for justifying inclusion (public interest)

What is data protection?

- Data protection is about ensuring people can trust you to use their data fairly and responsibly.
- If you collect information about individuals for any reason other than your own personal, family or household purposes, you need to comply.
- The UK data protection regime is set out in the DPA 2018, along with the GDPR (which also forms part of UK law).
- It takes a flexible, risk-based approach which puts the onus on you to think about and justify how and why you use data.
- The Information Commissioner's Office regulates data protection in the UK

General Data Protection Regulation (GDPR) : seven key principles

- **Lawfulness, fairness and transparency:** *identify valid grounds under GDPR (known as a 'lawful basis') for collecting and using personal data*
- **Purpose limitation:** *clarity about purposes for processing from the start*
- **Data minimisation:** *adequate, relevant, limited to what is necessary*
- **Accuracy:** *ensure personal data is not incorrect or misleading as to any matter of fact.*
- **Storage limitation:** *not keep personal data for longer than you need it (**research guidance)*
- **Integrity and confidentiality (security):** *appropriate security measures in place to protect the personal data you hold.*
- **Accountability:** *take responsibility for what you do with personal data and how you comply with the other principles.*

Questions???

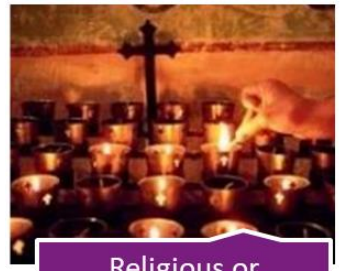
Personal data: what is it?

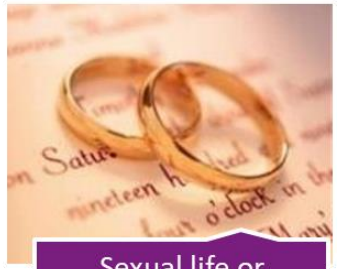
- any information relating to an identified or identifiable natural person ('data subject')
- an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as
    - a name
    - an identification number
    - location data
    - an online identifier
    - one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- The GDPR only applies to information which relates to an **identifiable living individual.** Information relating to a deceased person does not constitute personal data and therefore is not subject to the GDPR.

Personal data: special categories under GDPR

Personal data revealing

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership;
- data concerning physical or mental health
- data concerning sexual life or sexual orientation.
- processing of genetic data or biometric data for the purpose of uniquely identifying a person;





Personal data – additional considerations

- Research organisations that hold and use special categories of personal data must ensure that they have **a lawful basis to hold and use personal data and to hold and use special categories of personal data**

- **Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.**

- Information which is truly anonymous is not covered by the GDPR.

- If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

Pseudonymised data

- Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.
- The GDPR defines pseudonymisation as: *"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*
- Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately.
- Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations.
- However, pseudonymisation does not change the status of the data as personal data.

Anonymised data

- The GDPR does not apply to personal data that has been anonymised.

  "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject ***is not or no longer identifiable****. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

- In order to be truly anonymised under the GDPR, personal data must be stripped of sufficient elements that mean the individual can no longer be identified.
- If at any point reasonably available means can be used to re-identify individuals to which the data refers, data will not have been effectively anonymised but will have merely been pseudonymised.
- This means that despite attempts at anonymisation processing of personal data continues and is covered by GDPR.

Data controllers & Data processors: what are they?

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data controllers & Data processors: what are they?

- A data controller is an **organisation** which **determines the purposes and means of personal data processing**, even if the processing does not occur in the organisation.
- The Controller exercises **overall control of the processing** and is ultimately in charge of, and responsible for, processing.
- **Joint Controllers** are organisations that determine the purposes and means by which personal data are processed by jointly controlling processing for shared purposes.
- A **Processor** is an organisation which processes personal data on behalf of, and under the authority of, a Controller. Employees of a Controller are not Processors, as long as employees act within the scope of their professional duties.
- An organisation cannot be both a Controller and a Processor for the same data processing activity.

Data controllers

- decide to process personal data and the lawful basis for doing so
- determine the purpose(s) the data will be processed for
- choose what personal data to process and which individuals to process data about
- define how long to retain the data
- ensure that individuals are informed about the processing and decide how to respond to data subject rights requests. This includes ensuring patients are informed about how their data is used for research
- apply any interpretation, exercise of professional judgement or significant decision-making about the data processing

Data processors

Processors follow the Controller's protocol and agreements, but may decide:

- what IT systems or other methods to use to process personal data
- the details of the security measures to protect the personal data
- how it will transfer the personal data from one organisation to another
- how it will ensure it adheres to a retention schedule

A processor might wish to sub-contract all or some of the processing to another processor. For shorthand this is sometimes referred to as using a 'sub-processor', although this term is not taken from the GDPR itself.

Questions???

Lawful basis for data processing under GDPR

The lawful bases for processing are set out in Article 6 of the GDPR.

At least one of these must apply whenever you process personal data:

- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Data controllers and processors are required to provide information about the lawful basis for processing usually through a privacy notice.

Individual rights under GDPR

- The right to be informed
  - *Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.*
- The right of access
  - *Individuals have the right to access and receive a copy of their personal data, and other supplementary information.*
- The right to rectification
  - *The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.*
- The right to erasure
  - *The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.*

Individual rights under GDPR

- The right to restrict processing
  - *Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, you are permitted to store the personal data, but not use it.*
- The right to data portability
  - *The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.*
- The right to object
  - *The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.*
- Rights in relation to **automated decision making and profiling**.
  - *The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making* process.

Questions???

Assignment

To complete MRC Regulatory Support Centre Learning Management System training by creating an account on this page

https://byglearning.co.uk/mrcrsc-lms/login/index.php

- There you will find 10 e-learning modules which will reinforce your understanding of these topics
- These should take no more than 2-3 hours to watch and you are asked to do this over the coming week
- There is an associated quiz which you are asked to complete and pass (you can download a certificate to show you have done so)
- If necessary, you can use next week's tutorial time to complete this assignment or we can regroup and discuss any issues arising
- Today's slide set will be made available to you on QMPlus

Questions???