Understanding the implications of GDPR *(and new DP Bill)* on research

Dr Rachel Smith

Medical Research Council, Regulatory Support Centre

Briefing documents now available

Health Research Authority briefing documents

- Lawful basis
- Transparency
- Safeguards
- Data subject rights and exemptions

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/

NHS
Health Research Authority

How data is used in research…

- Usually requires ‘special category data’
- ‘Out of date’ data is routinely required
- Pseudonymisation of data is common
- Data flows can be very complex
  - Multiple sites
  - Not all data collected directly from data subjects
  - Collaboration and sharing of data encouraged (international)
- Re-analysis and meta-analyses encouraged
- Long term endeavor
- Legal avenues which enable the use of confidential patient information without consent (‘public interest tests’)
- Appropriate analysis and publication – account for all study participants (CONSORT guidelines)

How data is used in research…

- Usually requires ‘special category data’
- ‘Out of date’ data is routinely required
- Pseudonymisation of data is common
- Data flows can be very complex
  - Multiple sites
  - Not all data collected directly from data subjects
  - Collaboration and sharing of data encouraged
- Re-analysis and meta-analyses encouraged
- Long term endeavor
- Legal avenues which enable the use of confidential patient information without consent (‘public interest tests’)
- Appropriate analysis and publication – account for all study participants (CONSORT guidelines)

Tightly regulated

Preparing for implementation - Researchers' view

- Personal data
  - Pseudonymised data (common practice)
- Differentiating data protection from common law (confidentiality)
- Corporate nature of data protection legislation
- Jargon

Preparing for implementation – RECs view

- RECs make ethical decisions – the law is changing…not ethics
- Limited impact on RECs decision making
- Amendments – see HRA guidance

Common law (confidentiality)

Confidential information is…

- Information with degree of sensitivity associated with it, and
- Identifiable, and
- Not already in the public domain, and
- Given with the expectation that it will be kept confidential

Not the same as a secret…

Common law (confidentiality)

Confidential information is…

- Information with degree of sensitivity associated with it, and
- Identifiable, and
- Not already in the public domain, and
- Given with the expectation that it will be kept confidential

Not the same as a secret…

- Can be shared in line with reasonable expectations (i.e. no surprises)

- If public interest is great enough – disclosure is appropriate

General Data Protection Regulation (GDPR)

Additional requirements if collecting, holding, using ‘Personal Data’

Must be lawful, fair and transparent

No impact on common law

What is personal data?

- Structured information
- About or relates to a living person
- Identifiable (on its own or in combination with other information you are likely to have access to)

What makes data identifiable?

What makes data identifiable?

Year of birth

What makes data identifiable?

Gender

What makes data identifiable?

First part of post code

What makes data identifiable?

Place of birth

What makes data identifiable?

Year of birth

Gender

First part of post code

Place of birth

What makes data identifiable?

Year of birth	1965
Gender	Female
First part of post code	EH32
Place of birth	Bristol

What is personal data?

- Structured information
- About or relates to a living person
- Identifiable (on its own or in combination with other information you are likely to have access to)

Content and context

What is personal data?

- Structured information
- About or relates to a living person
- Identifiable (on its own or in combination with other information you are likely to have access to)

Test – ‘motivated intruder’ (what is reasonably likely?) – content and context

What is personal data?

- Structured information
- About or relates to a living person
- Identifiable (on its own or in combination with other information you are likely to have access to)

Test – ‘motivated intruder’ (what is reasonably likely?) – content and context

Control context with Agreements

What is personal data?

- Structured information
- About or relates to a living person
- Identifiable (on its own or in combination with other information you are likely to have access to)

Test – 'motivated intruder' (what is reasonably likely?) – content and context

Control context with Agreements

Pseudonymised data are personal!

Sub-set of personal data

‘Special categories of personal data’

- Roughly equivalent to ‘sensitive personal data’
- All (personal) health data
- Includes certain genetic data
- Almost all health research will involve the processing of special categories of data

GDPR

Lawful, fair and transparent

GDPR

Lawful – have a lawful basis

Fair and transparent

Lawful bases (GDPR)

Personal data (Article 6 GDPR)

- Public authorities – support task in the public interest
- *Non-public authorities – legitimate interest*
- *(Consent)*

Public interest – personal data (Article 6)

Universities should internally document justification for holding data under ‘public interest’, with reference to their public research purpose as established by statute or alternative (e.g. University Charter)

Lawful bases (GDPR)

Personal data (Article 6 GDPR)

- Public authorities – support task in the public interest
- Non-public authorities – legitimate interest
- *(Consent)*

Sensitive personal data ('special category' data) (Article 9 GDPR)

- 'Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)*
- *(Explicit consent)*

*Safeguards protecting the rights and freedoms of data subjects

Why do we get consent…

~~Lawful basis to collect, hold, analyse, and use personal data~~ (not likely)

- Supports ‘fairness’ (GDPR)
- Protection of autonomy (ethical)
- Common law (confidentiality – sharing confidential information within ‘reasonable expectations’)
- Clinical trial Regulations
- Human Tissue Act etc…

Researchers' view

- ? Lawful basis – unlikely to be consent
- ? Lawful vs fair and transparent
- ? Common law vs GDPR

MRC guidance

GDPR Preparation Guidance note 2 – current legal situation

www.mrc.ac.uk/regulatorysupportcentre ('News')

Ethics Committees' view

- ✓ Choice of lawful basis – only 'reputable' organisations can rely on public or legitimate interest as lawful basis – provides participants with some assurance
- ✓ Transparency and fairness – how individuals decide if they wish to their data to be included.
- ✓ Always looked at confidentiality

Lawful bases (GDPR)

Personal data (Article 6 GDPR)

- Public authorities – support task in the public interest
- Non-public authorities – legitimate interest
- *(Consent)*

Sensitive personal data ('special category' data) (Article 9 GDPR)

- 'Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)*
- *(Explicit consent)*

***Safeguards protecting the rights and freedoms of data subjects**

Minimum safeguards (GDPR / new DP Bill) - research

Processing personal data for health and social care research requires:

- Public / legitimate interest (Article 6)
- Technical and organisational measures, and
- Research will not cause distress/damage *or relate to a decisions about the data subject (unless approved medical research-REC)**,

For processing special categories of data for research:

- As above, and
- Test of specific public interest required –

  above that required in Article 6 *(public funding, REC approval, governance structures etc,*)

Minimum safeguards (GDPR / new DP Bill) - research

Processing personal data for health and social care research requires:

- Public / legitimate interest (Article 6)
- Technical and organisational measures, and
- Research will not cause distress/damage *or relate to a decisions about the data subject (unless approved medical research-REC)**,

For processing special categories of data for research:

- As above, and
- Test of specific public interest required – above that required in Article 6 *(public funding, REC approval, governance structures etc,*)

*Clause 19 DP Bill

Research – Article 5 (principles)

1(b)

- Limited purposes – scientific research use (as covered by safeguards) not an incompatible purpose

1(e)

- Storage limitation – scientific research (as covered by safeguards) can keep personal data long term

Minimum safeguards (GDPR / new DP Bill) - research

Processing personal data for health and social care research requires:

- Public / legitimate interest (Article 6)
- Technical and organisational measures, and
- Research will not cause distress/damage *or relate to a decisions about the data subject (unless approved medical research-REC)**,

For processing special categories of data for research:

- As above, and
- Test of specific public interest required –

  above that required in Article 6 *(public funding, REC approval, governance structures etc,*)

GDPR

Lawful – reputable organisation doing appropriate things

Fair and transparent – individuals can control if and how their data is used

Organisation + personal control = GDPR fair, lawful and transparent

Researchers' view

- ✓ Know about and follow university policies (IG, etc)
- ✓ If it's not working for you – speak to someone…
- ✓ Pseudonymise data (standard practice now)
- ✓ Only use identifiable data when you really need to

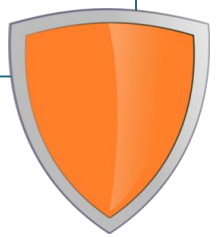
- ? Confusion around roles of Research Governance staff, DPO, IT staff and HRA
- ? The details are not easy to understand
- ? Public interest – how many different levels?
- ? Lawful, fair and transparent – consent?

Ethics Committees' view

- ✓ RECs have always made a public interest judgement – level of decision unchanged
- ✓ Storing research data long term – ethical imperative to do so provided it is safe (maximise the use of data including making data available for meta-analyses)

Transparency

- High level corporate information
  - Include: We hold and use personal data to support scientific research
- Research group / department information
  - Poster in clinic waiting room
  - Departmental website etc
- Study specific information
  - Participant information sheet / consent form



Should include

- Who is the Data Controller
- Why the data is being processed
- Any (significant) risks involved
- Safeguards put in place to limit risk
- Details of how people can exercise their rights etc
- Legal basis

Information requirements vary if data obtained directly from data subject vs from a third party

Should includ

Complex data flows – controller vs processors

- **Who is the Data Controller**
- Why the data is being processed
- Any (significant) risks involved
- Safeguards put in place to limit risk
- Details of how people can exercise **their rights**
- **Legal basis**

Public interest / research

What rights will participants have – which exemptions / safeguards are you going to use?

In quireme
d s from a

Should includ

Complex data flows – controller vs processors

- **Who is the Data Controller**
- Why the data is being processed
- Any (significant) risks involved
- Safeguards put in place to limit risk
- Details of how people can exercise **their rights**
- **Legal basis**

Sponsor / co- sponsor?

Public interest / research

What rights will participants have – which exemptions / safeguards are you going to use?

In quireme
d s from a

Ethics Committees' view

- ✓ Consent – part of transparency and fairness
- ✓ Will the average potential participant understand the PIS (or other information e.g. posters) provided?
- ✓ RECs will not see all transparency information
- ✓ Support generic use of data

Research participants' view

- Difficult concepts to understand
- Language and understanding

  https://understandingpatientdata.org.uk/
- Confusion - different Data Controllers for different purposes…?
- Confusion – also Patient Notifications (required by Confidentiality Group if accessing NHS / social care data without consent)
- Generic use of data

Rights and exemptions (GDPR and new DP Bill)

Subject rights (exemptions are available if processing for research purposes)

- Informed
- Erasure of data
- Portability of data
- Objection to processing
- Access by data subject
- Rectification of data
- Restriction of processing

Rights and exemptions (GDPR and new DP Bill)

Subject rights (exemptions are available if processing for research purposes)

- Informed
- Erasure of data
- Portability of data
- Objection to processing
- Access by data subject
- Rectification of data
- Restriction of processing

*Exemptions from each right requires different combinations of further safeguards to be in place. These are in addition to the minimum safeguards

Minimum safeguards (GDPR / new DP Bill) - research

Processing personal data for health and social care research requires:

- Public / legitimate interest (Article 6)
- Technical and organisational measures, and
- Research will not cause distress/damage *or relate to a decisions about the data subject (unless approved medical research-REC)**,

For processing special categories of data for research:

- As above, and
- Test of specific public interest required –

  above that required in Article 6 *(public funding, REC approval, governance structures etc,*)

Exempt from rectification if

Likely to render research impossible or to seriously impair achievement of research objectives

Exempt from restriction of processing if

Likely to render research impossible or to seriously impair achievement of research objectives

Exempt from informed if

Personal data obtained from a third party AND

Likely to render research impossible or to seriously impair achievement of research objectives

OR

Disproportionate resources required

Exempt from access if

Likely to render research impossible or to seriously impair achievement of research objectives,

and

Research results will not to be published in an identifiable form

or

Health professional has the opinion that access would cause harm

Exempt from erasure if

Likely to render research impossible or to seriously impair achievement of research objectives,

and

Consent is NOT lawful basis

Exempt from objection if

Likely to render research impossible or to seriously impair achievement of research objectives,

and

Lawful basis is ‘public interest’

Or

Data controller can show that processing is necessary to support a task carried out in the public interest

Exempt from portability if

Not using consent or fulfillment of a contract as your lawful basis

Researchers' view

?!!?*?

- ✓ Do not make any decisions on your own
  - ✓ DPO / Research Governance / HRA input
  - ✓ Know and follow policy

Research participants' view

- Equal rights for all…? Only fair
- Joined up and explained clearly…
  - What does withdrawal mean…?

Keeping up to date…

Guidance

HRA guidance

What is the impact on REC review? – Not much!

What is a substantial amendment?

What data issues are considered as part of HRA assessment?

https://www.hra.nhs.uk/

MRC guidance

Interpretations of the law for researchers and research managers (as simple and practical as possible!)

http://mrc.ac.uk/regulatorysupportcentre

MRC Medical Research Council

Regulatory Support Centre

www.mrc.ac.uk/regulatorysupportcentre