GDPR – myth busting

Dr Janet Messer
Director of Approvals Service, HRA

NHS
Health Research Authority

NHS
Health Research Authority

GDPR what's it for?

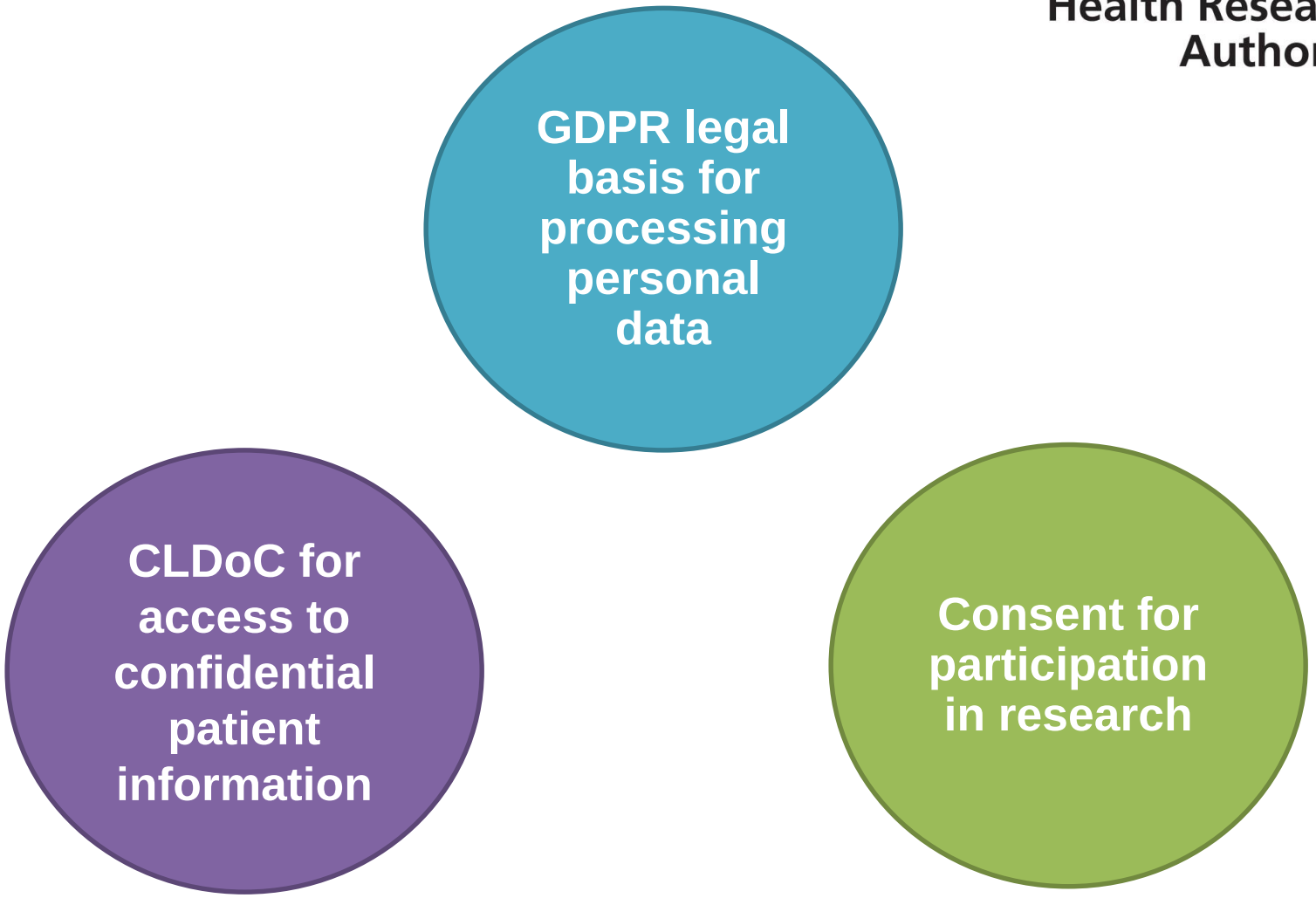
Health Research Authority

Health Research Authority

What has changed?

- ✓ GDPR
- ✓ Data Protection Act 2018/ member state legislation
- ✘ Common law duty of confidentiality/ European Convention Human Rights
- ✘ Ethics – privacy and confidentiality

NHS
Health Research Authority



Health Research Authority

GDPR

- **Lawful**
- Transparent
- Fair

GDPR and research

Health Research Authority

- GDPR and DPA specifically drafted to not hinder research
- Data can be retained for research
- Data can be used for multiple research purposes

Health Research Authority

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

Pseudonymised data – could be personal!

UK approach – legal basis

Health Research Authority

Personal data

- Legitimate interest/ task in the public interest
- *Consent – if other bases not available*

Sensitive personal data ('special category' data)

- 'Processing is *necessary* for scientific research purposes' subject to safeguards
- *Explicit consent – if other bases not available*

Why not consent as legal basis?

Where processing is based on consent the data subject enjoys a number of rights linked to consent:

- The right to data portability
- The right to withdraw consent
- The right to erasure

This does not work for research!

But it doesn’t mean we don’t seek consent...

Health Research Authority

Problems with consent

"if the controller chooses to rely on consent for the collection of research data they may do so, as long as they explain that retention and analysis of the data collected is on the separate basis of legitimate interests - whether or not the individuals withdraw their consent."

UK Information Commissioner's Office

Why do we get consent for research…

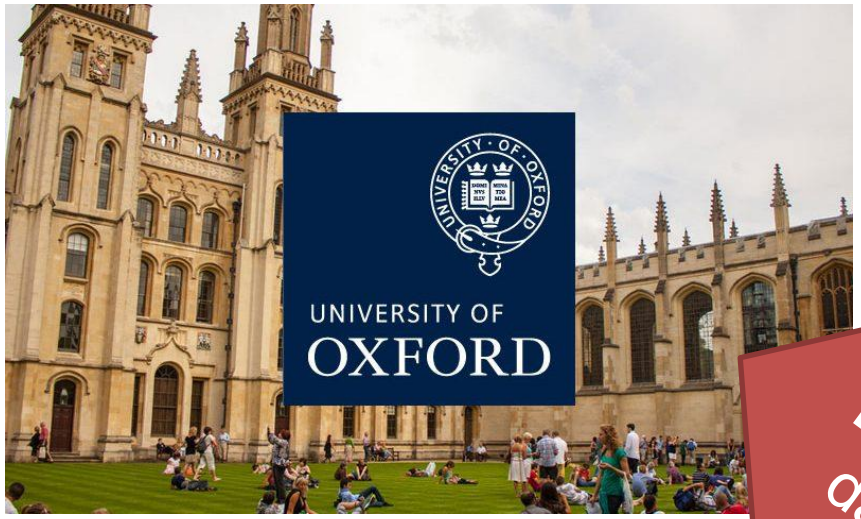
~~Lawful basis to collect, hold, analyse, and use personal data~~

- Part of fairness
- Protection of autonomy (ethical)
- Protect confidentiality – sharing confidential information within ‘reasonable expectations’
- Human Tissue Act
- Clinical Trial Regulations etc

NHS
Health Research Authority

Who is the data controller?

Who is the data controller?



Research data =
questionnaires + test results

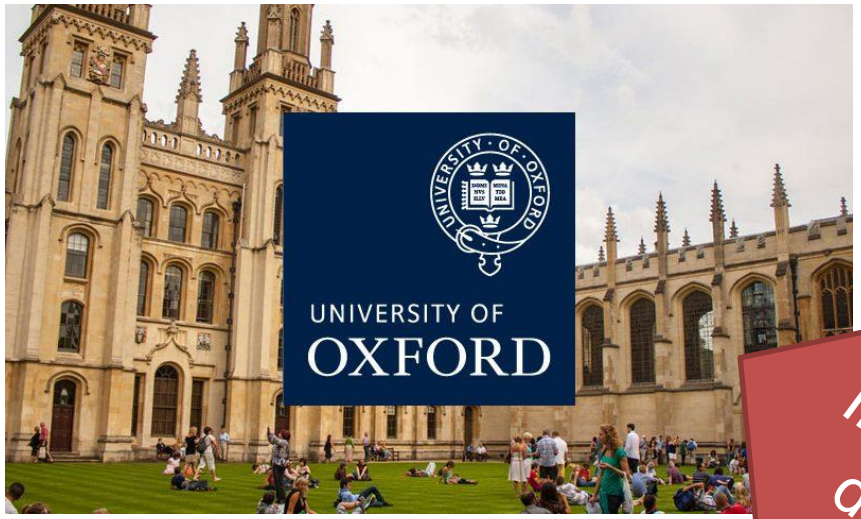
Site = processor

Direct data

Sponsor = controller

Who is the data controller?

Research data = medical records



Sponsor = controller

Indirect data

Site = controller

UK approach - Controller-processor agreement

- Requirement to legally bind processor
  - GDPR compliant mNCA published
  - GDPR compliant mCTA in development
  - Arrangements for complying for ongoing processing – with ICO lawyers

Health Research Authority

GDPR

- Lawful
- **Transparent**
- Fair

Health Research Authority

Transparency

- Corporate responsibility
- Privacy notice
  - Provision of a hierarchy of information
  - High level corporate information…
  - Department level…?
  - Research group level…?
  - Study level – consent materials (when appropriate)
  - Accessible – understandable and *available*

Health Research Authority

Health Research Authority

GDPR

- Lawful
- Transparent
- **Fair**

GDPR Safeguards

For processing all personal data:

- Technical and organisational measures eg:
  - security
  - data minimisation

For processing special categories of data for research:

- Technical and organisational measures
- Test of specific public interest required, eg REC/CAG review

But we should already have…

- Security arrangements and encryption
- Data minimisation
- Policies and procedures
- Control over access

…shouldn't we??

Privacy Impact Assessments

Health Research Authority

- Health research already takes place within a context of established arrangements for sponsor oversight and for use of personal data
- Study wide review through HRA Approval will highlight considerations for local decision
- Host sites are not required to undertake Impact Assessments for individual studies
- There are limited number of situations where a Data Privacy Impact Assessment is legally required under GDPR – see guidance

Health Research Authority

Pseudonymisation

- Act of anonymising/pseudonymising is processing – needs legal basis
- Pseudonymised data is NOT necessarily personal data
- Need to consider common law duty of confidentiality – WHO is pseudonymising

Health Research Authority

Preventing re-identification

- Stewardship
- Restrictions on any recipients as to purpose and any further use
- Contracts
- Technical measures
- Professional codes

- Watch out for onward sharing!

Sponsors and pseudonymisation

- Interventional studies – data usually coded at site
- Sponsor is still processing personal data – site is processor
- Safeguard is that sponsor does not receive personal data

Health Research Authority

Sponsors and pseudonymisation

- Data studies – is someone else coding/ linking personal data for your study?
- Controller-controller relationship?
- If already pseudonymised are there sufficient controls that prevent identification – may not be personal data

Health Research Authority

Post-study data sharing

- Good scientific/ ethical rationale for sharing study data
- If have legal (GDPR) and legitimate (CLDoC) basis for access to data then can anonymise for future use
- Research not regarded as incompatible with original purpose
- Sufficiently anonymised (with controls) is not personal data or confidential patient information
- Ethically – good practice to inform

Health Research Authority

Common law duty of confidentiality

- ‘Reasonable expectations’
- Definition of confidential patient information
- Definition of care team
- S251 support to set aside common law
- Patient notification and objection (objection is not the same as opt out!)

NHS
Health Research Authority

Applying the national data opt-out to research

Data is anonymised

Researchers only access data that is compliant with the ICO 'Anonymisation: managing data protection risk' code of practice. Data is not classed as confidential patient information
and it would not be possible to cross-check the opt out list.

NDOP does not apply

Specific Consent in place

The national data opt-out does not apply when participants have given specific consent for their data to be used for research, regardless of whether consent was given before or after the patient registered a national data opt-out. There is not need to cross-check the opt out list.

NDOP does not apply

Research involving confidential patient information without consent

Research relying on s251 support through CAG is subject to national data opt-out. CAG can override the opt-out, but this will only be in exceptional circumstances. Research will usually have additional patient opt out required as a condition of support.

NDOP applies

Health Research Authority

Health Research Authority

HRA.queries@nhs.net