General Data Protection Regulation (GDPR) – Preparations for implementation

Guidance note 1

The MRC Regulatory Support Centre has produced this guidance note to help Research Governance Managers, and others who have governance oversight for medical research within organisations, to prepare for the implementation of the General Data Protection Regulation (GDPR) in May 2018. This is the first in a series of GDPR – Preparation for implementation guidance notes. Please check www.mrc.ac.uk/regulatorysupportcentre **'News'** for future releases.

At this stage your focus should be on awareness of the data your organisation holds to support research. Researchers, Data Managers, Trial Managers, etc. may also find this document useful. However, we would recommend that interested individuals (e.g. Research Governance Managers and/or Researchers etc.) work with the appropriate management oversight functions (i.e. your organisation's Data Protection Officer (DPO)), to ensure coherent and organisation-wide actions are taken, where they are needed.

The GDPR:

a. Should have little impact on research that conforms to current good practice,
b. Requires organisations to do some preparative work before implementation, to ensure compliance (covered in this guidance), and
c. Requires the government to resolve some research specific details.

Although the law in the UK, as it relates to personal data, is changing with the GDPR, there are no changes to the common law (i.e. confidentiality).

The Information Commissioner's Office (ICO) is producing guidance to aid implementation of GDPR in general. We prepared this note in July 2017, and updated it in August, when research derogations and other research specific details of the GDPR were still to be confirmed. Once these details are known, we will work with the Health Research Authority (HRA) and others to produce further guidance for the research sector.

As many of you will not yet be familiar with the terminology used in the GDPR, in this guidance note we use common terminology used in medical research and the current Data Protection Act. We have provided links to definitions used and existing guidance where appropriate.

1. Does your organisation have a Data Protection Officer (DPO)? Are they aware of the personal data (including sensitive personal data) held to support research?

Research Governance leads should contact your DPO and work with them to ensure that your organisation is GDPR ready. Your DPO is responsible for legal compliance including

the provision of an accessible privacy notice. The questions in this guidance note should facilitate discussions.

2. What personal data does your organisation hold for research? How much is sensitive personal data?

Data are personal data when they relate to or are about a living person, and are identifiable (i.e. identification is 'reasonably likely'). For a definition see: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Sensitive personal data are personal data that conform to one of the categories outlined in Part 1 section 2 of the Data Protection Act (see: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/). All health related personal data are classified as sensitive personal data.

Be aware that pseudonymised data are classed as personal data. Pseudonymised data are personal data where identifiers are physically split and stored separately from the rest of the dataset; but kept within the same organisation. For more information see ICO Anonymisation Code (see: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf).

3. Of this personal / sensitive personal data – which data do you have explicit consent to hold and use?

The GDPR introduces requirements for explicit consent, as opposed to implied consent (see below). The ICO will be producing general consent guidance, following the GDPR consent guidance consultation that closed earlier this year, and the HRA is expected to produce guidance specifically for health research. We believe that for most medical research, explicit consent obtained in line with current good research practice will be practically unaffected by the implementation of the new Regulation (this includes broad consent for medical research). We also believe that re-consent for existing studies will not be needed in most cases.

For more information on good practice in this area, please see HRA Consent and Participant Information Sheet Preparation Guidance at: http://www.hra-decisiontools.org.uk/consent/.

Questionnaire studies and implicit consent

Be aware that there are a few research scenarios where implicit consent may be standard practice: in particular, consent to take part in questionnaire studies. It is now increasingly common to enable participants to indicate their agreement to take part in such studies by completing and returning the questionnaire. Any personal / sensitive personal data collected in this way, is collected with **implicit** and not explicit consent. You should try to determine what personal and what sensitive personal data your organisation is currently holding with implicit consent, as well as with no consent at all (see 4 below). The government still has to determine further detail around the legal bases public authorities will have to hold such data.

Children and young people

The GDPR provides additional protections when consent is being sought to collect and use personal and sensitive personal data relating to children and young people. Again, we believe that if your organisation is holding personal or sensitive personal data relating to children and young people with explicit consent as described in current HRA guidance, there

will be no practical change as a result of the implementation of the new Regulation with respect to consent. Be aware that your Data Protection Officer will have to ensure that your organisation's privacy notice is accessible (i.e. understandable to older children).

4. Does your organisation currently hold or use personal / sensitive personal data without explicit consent?

This could be data that:

a. Have been released to you with support from the Confidentiality Advisory Group (i.e. with '251 approval') or with approval from other responsible bodies within the Devolved Administrations; or
b. Were collected with implied consent, for example in some questionnaire studies or where data are collected online and you are holding any personal identifiers (e.g. Internet Protocol (IP) address etc.); or
c. Were collected with consent that would not conform to current accepted good research practice as outlined by the HRA (e.g. consent was taken some years ago etc.; see http://www.hra-decisiontools.org.uk/consent/).

The GDPR continues to allow personal data to be used for medical research without consent in specific circumstances: however, the status of some of these still need to be resolved by government. You have no actions to take now, other than to be aware of what personal / sensitive personal data your organisation is holding which fall into these categories.

5. Does your organisation currently have a privacy notice that specifically mentions the use of personal / sensitive personal data to support research? Is this notice freely available to the public?

Privacy Notices must currently be provided by all organisations that hold personal data (i.e. by all Data Controllers). Your organisation's Data Protection Officer (DPO) produces this notice and ensures it is complete. For more guidance on privacy notices see https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Your DPO may need to make changes to the current Privacy Notice to reflect how personal data are collected and managed for research, along with other more general changes to reflect how your organisation uses other personal data in light of the GDPR.

Be aware that a Privacy Notice is not the same thing as Patient Notification. The Confidentiality Advisory Group (CAG) require Patient Notification (under the Control of Patient Information Regulations) when confidential patient information is disclosed under Section 251 approval.

6. Does your organisation have an established process / processes to handle withdrawal of consent?

It is likely that many research groups will have thought about this issue and will have put a process in place. They may have already informed research participants of their options in terms of withdrawal of consent. If no process is currently in place, start planning with your DPO how an effective withdrawal process could be put in place to comply with the deadline.

7. Does your organisation currently send or receive personal data to collaborators etc. within or outside the European Economic Area?

It would be useful for you to know which projects involve international transfer of personal data, both:

- between the UK and countries within the EEA; or
- between the UK and countries outside of the EEA. The following ICO guidance is relevant here: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/

In your considerations, you should exclude all robustly anonymised data: that is data anonymised in line with ICO Anonymisation Code: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.