Current thinking on Controllers and Processors in health research

This guidance was developed by the MRC Regulatory Support Centre in collaboration with the HRA, NHS Digital, CPRD, PHE and eDRIS. This guidance is for researchers, research governance teams, Data Protection Officers and legal/contracts teams.

Data protection legislation details organisations' responsibilities and obligations when processing personal data. This includes determining whether they are Controller or Processor for all of their data processing activities. The Information Commissioner's Office sees data protection as an organisational responsibility, and as such, researchers should not make this decision alone. Although this guidance focusses on data protection, other (legal) requirements may apply (for further information please see mrc.ukri.org/regulatorysupportcentre).

Definitions

A **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.

A **third party** is any person or organisation, other than the data subject, Controller, Processor, or persons authorised by a Controller or Processor to process personal data.

Health data and research

It is important to distinguish between an organisation's own data processing activities (i.e. when it is a Controller) and data processing carried out on behalf of other organisations (i.e. when it is a Processor). For example, NHS organisations are Controllers of data processing associated with the care of their patients, but may not be Controllers when that patient data is used for research.

When research is led by an NHS organisation, the NHS organisation is a Controller. When research is led by a non-NHS organisation, such as a University, the University is a Controller. When Universities lead research involving NHS organisations, the NHS organisations are Processors, as they are following the University's protocol and processing data on behalf of the University (the Controller). Even if data processing does not take place in the University, the University is a Controller.

In this context, Controller relates to data protection only. Other research considerations, such as intellectual property rights, publications rights, duty of confidentiality, are not relevant when considering whether an organisation should be a Controller.

In addition to data protection legislation, identifiable health information is subject to the common law of confidentiality, and therefore confidential information can only be disclosed within participants' reasonable expectations. NHS and other research organisations are responsible for ensuring that the duty of confidence is upheld when sharing confidential information for research. This is separate to data protection. For more guidance on confidentiality in research please see our guidance on confidentiality.

How to identify whether an organisation is a Controller or a Processor?
A Controller determines the purposes and the means of the data processing. As such, a Controller exercises overall control over the 'why' and the 'how' of the data processing. For health research, the Sponsor will be a Controller, as the Sponsor determines the 'why' and the 'how' of the research, even when processing does not take place within the Sponsor's organisation.

However, this distinction is not always clear in collaborative research as responsibilities are generally shared between organisations. For example, the fact that one organisation processes personal data from another organisation does not necessarily mean that they are a Processor. They could be a Controller in their own right, depending on the degree of control they exercise over the data processing i.e. a research project could have a single Sponsor and several Controllers.

Although not exhaustive, below are some of the issues organisations should consider when determining who is Controller or Processor. This is an organisational responsibility (usually made by a Data Protection Officer) and shouldn't be made by research teams.

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. For example, being assured that NHS organisations have told patients about how their data is used for research
- apply any interpretation, exercise of professional judgement or significant decision-making about the data processing

The more of these kind of decisions an organisation takes, the more likely it is to be a Controller. For research, these decisions will be described in the protocol and detailed in the Controller / Processor agreement.

Joint Controllers

- define a common objective with another Controller regarding the processing
- process the same set of personal data and for the same purpose, as another Controller
- have common information management rules with another Controller

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

Example 1

A University sponsors a project to follow-up research carried out 10 years ago. The protocol involves sending participants' NHS numbers to a central NHS data source. The central NHS data source will link the NHS number to follow-up health data and send a dataset to the University.

The University and central NHS data source discuss the research. The central NHS data source decides that the data linkage does not require their significant expertise or interpretation and can be achieved by following the protocol. The Sponsor is a Controller as they have determined the purposes and means of processing personal data for the research i.e. they have decided:

- to process personal data and the lawful basis for doing so
- the purpose of the processing and how long to retain data for
- which items of personal data to process and which individuals to process data about

The central NHS data source is a Controller for processing data that it has collected for routine purposes. However, for the research it is a Processor, because the University, not the NHS data source, has decided what data to process and why and which individuals' data will be processed.

Example 2

NHS Organisation A sponsors research that involves prospective collection of personal data from patients at NHS Organisation B, and retrospective collection of pathology results of these patients at NHS Organisation C. Anonymised data is then sent to NHS Organisation A.

NHS Organisation A is the Sponsor and therefore a Controller, even though no processing takes place within NHS Organisation A. NHS Organisations B and C are Processors as they will follow NHS Organisation A's protocol. NHS Organisations B and C are Controllers for processing the data that they hold for care. However, for the research they are Processors, as they process and provide the data that NHS Organisation A has decided it needs for the research.

Example 3
Researchers at a University organise a multi-site research project carried out with local NHS Organisation A. The University and NHS Organisation A routinely Co-Sponsor research. The protocol states that participants will be identified at a number of NHS sites and at Participant Identification Centres (PICs). Patients will be invited to undergo physical assessments and have data collected. Data will then be sent to the University.

The University and NHS Organisation A are Co-Sponsors and Joint Controllers, agreeing and documenting their respective responsibilities. The NHS sites and the PICs only process personal data at the request of the Sponsors by following the protocol, and their decisions are limited to the methods of data processing and how to transfer data to the Controllers. The NHS sites and PICs are therefore Processors. The exception to this is the site at NHS Organisation A, which as a Joint Controller, cannot also be a Processor.

Example 4
Researchers at University A obtain funding for a multi-site drug trial. University A contracts a Clinical Trials Unit (CTU) at University B to carry out the research. The CTU designs the trial protocol, including which people will be approached for recruitment, what data will be collected, sample sizes, how the results will be interpreted and how to handle data subject rights requests.

University A, as Sponsor, has decided to process data and for what purpose, and is therefore a Controller. The CTU does not process any personal data (this being retained at the sites), but the CTU has designed the protocol and therefore determined the detail of what personal data to collect and from whom. In practice, the CTU decides how long sites will retain the personal data, whether to share any data, and when data subject rights apply. In this situation it is likely that University A and University B (where the CTU is based) will be Joint Controllers, with an agreement documenting their respective responsibilities. The trial sites would be Processors as they will not be involved in any significant decision-making and will only process data by following the protocol.

Summary
Organisations must determine if they are a Controller or a Processor for research projects that they are involved in. For the vast majority of health research, we expect that the Sponsor will be the sole Controller. Joint Controllers are logical for Co-Sponsored research and for research where CTUs make significant decisions about processing. However, having Joint Controllers and a single Sponsor needs careful management to ensure responsibilities are clear and that the Sponsor has adequate oversight. Determining Controller / Processor status does not absolve any organisations involved in research from other responsibilities, such as the common law of confidentiality.

Further details on this topic can be found in the ICO guidance on Controllers and Processors.