Controller Model Statement

1. Introduction

All organisations in the Connecting Care Partnership are individually Controllers but, depending on their relationship with the data in Connecting Care, they may be a:

- Joint Controller
- Controller in Common
- Processor

These definitions are based on the Information Commissioner's Office (ICO) guidance on terms used in previous legislation (Joint Data Controller/Data Controller in Common and Data Processor), and the definitions in the General Data Protection Regulations (GDPR).This guidance is still relevant, until the ICO publishes new guidance based on the current legislation.

The Controller determines the purposes for which, and the manner in which, personal data is processed. They can either do this on their own, or jointly, or in common with other organisations.

This statement applies to all Controllers both 'Joint' and 'In Common' and Processors that are a part of the Connecting Care Partnership. These are official terms and are agreed as:

- A Joint Controller is defined in Article 26 of the GDPR, as when two or more controllers jointly determine the purposes and means of processing
- A Controller in Common is an organisation that simply accesses data but does **not submit** data, as per the ICO definition.[1] These organisations are processing the common dataset for their individual purposes, and will often be sponsored by a stakeholder organisation.
- A Processor is any person (other than an employee of the data controller) who processes the data on behalf of the Controller. In the Connecting Care context, this is currently South Central & West Commissioning Support Unit (SCW) and University Hospital Bristol (UHB).

[1] Applies where two or more persons share a pool of personal data that they process independently of each other.

(This document uses specific legal terminology, to explain the relevant legal concepts.)

All Connecting Care stakeholder organisations jointly define and agree on the following:

- The security features within the portal
- Access control
- User management
- Usage limitations of the data contained in the portal
- Core shared purposes
- The manner in which the data is processed

There is an obligation on all Connecting Care stakeholders to promote the use of Connecting Care.

All Joint Controllers decide:

- What data that belongs to their organisation should be made available in Connecting Care
- What levels of access to information should be assigned to a Connecting Care role
- The purposes that information accessible via Connecting Care can be used for
- Whether a sponsored organisation should be authorised to access Connecting Care

All Controllers in common are not permitted to:

- Access the system unless they agree with the purposes and security requirements stipulated by the stakeholder organisations
- Have decision making powers over the design and operation processes associated with the system.
- They may suggest the access control and data they need, but the final decision will reside with the Connecting Care Joint Controllers

2. Individual Controllers

Each Controller is bound by the requirements placed on them under the General Data Protection Regulations and retains individual responsibility for:

- **Their own data.** Up until an organisations dataset is combined with any others for the purpose of the Connecting Care portal, it is the responsibility of the individual data controller.
- **The right to share.** Any individual Controller has the right to share or not to share. The information shared on the portal will be decided by the Controller and they have the right to not share any data item where they are not convinced of the need to share.

Or where they feel the access control within the portal is not sufficient to afford such data adequate protection. For example, where there is an identified need to share, but perhaps on a limited basis that the security in Connecting Care is not designed for at the time of sharing. The information should be shared by other means or by Connecting Care in time with system improvements.

- **Failure to provide accurate data.** Where an incident related to the submission of inaccurate data occurs, the source will be traced and the liability will reside with the providing party/ies.
- **Inappropriate use of the Connecting Care portal by staff.** Any incident of inappropriate use or disclosure of information viewed via the portal by staff, where there is no legal basis for the use/sharing, will be the liability of the individual Controller that employs that member of staff.
- **Informing**. There are duties placed on Controllers and Processors to inform the public of all the processing activities they carry out on the personal data that they control, as laid out in Article 13 & Article 14 of the GDPR. This duty can be met by using materials provided as well as considering additional ways of informing such as privacy/transparency notices and their own informing materials.
- **Data subject rights.** All Stakeholders shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under the GDPR, in particular with regards to the exercising of the rights of the data subject. Article 26.
- **Identifying an IG resource to attend the IG Leads Group**. Each Controller is required to identify an IG resource to attend the monthly IG Leads meetings and comply with the Information Governance Group's current Terms of Reference.

3. Joint Controller and Controllers in Common liabilities

The joint controllers are jointly liable for the following. Please note that this is based on the Connecting Care Programme risk register:

- **Any inappropriate access**. Where the jointly agreed security model/access controls were found lacking in preventing a user accessing data they did not need to see. Please note, this **does not** include instances where an individual controller's employee has deliberately circumvented access controls by sharing of access credentials.
- **Contravention of Articles 44 to 50 of the GDPR/**. Any processing of data by the Connecting Care portal that takes place outside of the European Union (EU) and approved listed countries.
- **Acting upon inaccurate data.** Where a user has acted upon inaccurate data by any party where the error is a result of failure in the Connecting Care System e.g. patient matching.

4. Processor Liabilities

The Processor/s have general liabilities as laid out in Article 28 of the GDPR and have specific liability in respect of failures and issues relating to the following:

- **Availability of the system.** In relation to the main system, and networking that links the system to the wider networks, the data processor will be liable for availability. Please note that this **does not** include were unavailability has been caused by network issues within an individual organisation e.g. if one external organisation can access the system, it will be considered as up and running.
- **Contravention of Articles 44 to 50 of the GDPR/**. Any processing of data by the Connecting Care portal that takes place outside of the EU and approved listed countries.
- **Opt out request not actioned.** The impact of an individual's data not being removed from the portal, when it has been requested by them. Including if the portal is found lacking in functionality.
- **Inadequate central processes.** Any incidents that occur as a result of inadequate central processes to manage user accounts. This applies to all agreed and centralised management processes. Please note this **does not** include were an incident is the result of an individual data controller not performing the relevant process e.g. failing to inform, in a timely manner, central management of a leaver.
- **External hacking threats to the main system.**
- **Resilience/back up of the system.**

The Controller Model Statement has been agreed by the Connecting Care Information Governance Group in July 2018.

Version	Date
4.4	10.07.18