Information Governance FAQs

How is access to the system secured?
All authorised users of Connecting Care will have a user name and password. A secured N3 connection is required to access Connecting Care.

Does everybody see the same types of information?
No, Connecting Care is based on a user's role. This determines their level of access to different types of information. There are a number of functions within the system that can be used to limit access to an individual's data. These range from having no access, to limited access through to full record access.

How is access to records managed?
Information materials have been created across all participating organisations to publicise the programme to patients. These items have been designed to inform individuals about the programme in general and form a basis of implied consent and offer an opt-out from their information being accessed via the system. All access that is granted is appropriately authorised by the partner organisation.

Can an individual 'opt-out' of Connecting Care?
Yes, if an individual does not want a Connecting Care Record to be accessible to relevant health and care staff delivering care to them, then there is an 'opt out' form available via the Connecting Care website for downloading and passing to the individuals. They will receive written confirmation their request has been actioned. Without the form individuals must contact Patient Advise and Liaison Service (PALS), who will inform Connecting Care.

Can an individual opt back in to Connecting Care after opting out?
Yes, they can do so by contacting PALS.

What are the data sharing arrangements for Connecting Care?
Each organisation that participates in Connecting Care, as either a provider of data, a user of data or both, is required to sign up to our information sharing agreement. This defines what data is shared, for what purpose and how access to the data is managed. It is compliant with the data sharing code of practice published by the Office of the Information Commissioner.

Is there an audit trail?

The Connecting Care system has full audit trail functionality. How and when individual data is accessed and by whom is captured within the systems audit trail. Reports can also be generated for review and identification of potentially suspicious activity.

Personal responsibilities

- **Do not share log on credentials**. If you believe a colleague needs access to Connecting Care, ask them to apply to be a user. If they are locked out or have forgotten there details they should either reset their own password using the self-service option if set up or contact their local service desk.
- **Think before you print**. If you need to print from the Connecting Care system ensure this is handled securely, throughout transportation, distribution and destruction.
- **Do not access family or friends records.** Connecting Care must only be used for work related purposes, where you have a justified reason to access data on individuals. All use is monitored and disciplinary/legal action will be considered in relation to any inappropriate use.
- **Do not leave yourself logged into Connecting Care.** Remember to lock your screen when you are away from your desk and log out of Connecting Care when you have finished.
- **Appropriate sharing**
  If you are sharing information from the Connecting Care portal please ensure you have a legal gateway to do so.

Further Information

If you have further Information Governance related questions please ask your organisation's Information Governance Lead.

Further information can be found on the Connecting Care Public website -

https://www.connectingcarebnssg.co.uk/