Data Security and You

In order to comply with the consent that 100,000 Genomes Project participants have given, it is of paramount importance that users of the Research Environment take the security of the platform and its data very seriously. Genomics England will not tolerate users abusing their access, breaching any safeguards put in place, or otherwise endangering the security of confidential participant data.

Genomics England can ban the institution and all their researchers from accessing the Research Environment if a user deliberately breaches the security of the system. Any deliberate attempt by a researcher to reveal the identity of a 100,000 Genomes Project participant is a breach of the Data Protection Act, and could result in a criminal charge or heavy fine.

Your Security Obligations

Having completed Information Governance training prior to getting access to the research dataset you should remember that:

1. You must **not** share your login details with others;
2. Only carry out research on the research dataset - clinicians with access to the identifiable clinical data should join GeCIP to carry out research;
3. Do **not** 'screenshot' the Research Environment or otherwise shortcut the Airlock;
4. Prepare any material for airlock import or export with consideration of its impact on data security (see the guidelines in the airlock section of this site);
5. Do **not** carry out any activity on 100,000 Genomes Project research data that may reveal any participant's identity;
6. Inform Genomics England Service Desk immediately if you:
    a. observe other users endangering the security of the environment or dataset;
    b. fear you have breached the security of the environment or dataset;
    c. think your login details have been compromised.

The following is taken from the Genomics England IG Confidentiality and Data Protection Policy which can be found in the Library and Resources section of the website ⚠.

Data Protection

The *Data Protection Act 1998* (The Act) came into force in March 2000. The Act sets out standards which must be satisfied when processing data relating to living individuals. Processing includes recording, obtaining, holding, using, generating derived data, analysing, disclosing and destroying personal data. The Act covers information on any media stored on computers and also within manual records.

Under the Act an individual has a right to see personal information held about them. This is normally referred to as a Subject Access Request (SAR).

The Act regulates the use of two types of data, “personal data” and “sensitive personal data”. The definitions of those under the Act are as follows:

- Personal data is information which can directly identify a person – in which the person is the focus of the information and which links that individual to details that would be regarded as private (e.g. name and private address, name and home telephone number etc.). This definition also includes members of staff and contractors.
- Sensitive personal data is personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Where staff are processing personal data, whether permanent, temporary or contractors then they are responsible for ensuring that the 8 principles of this Act are adhered to. These are as follows:

1. Personal data shall be processed fairly and lawfully.
2. Personal data should be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up-to-date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act. Under this principle data subjects have the right of access to information held about them.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appropriate care must be taken to protect personal data or sensitive personal data when it is transferred in whatever format. The Data Protection Act 1998 (DPA) requires that:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data.*

The British Standard for Information Security (BS7799) and the International Organization for Standardization Information Security standard ISO27001 also require that appropriate controls are in place to maintain the security of information exchanged with external organisations, requiring procedures and standards to be established to protect information in transit.

These procedures must be applied at all times whenever personal data or sensitive personal data is transferred either within Genomics England, or externally. Methods of transfer refer to the transfer of information via any form, examples include:

- Electronic file transfer
- Email
- CD or DVD
- USB Memory Sticks
- By Post / Fax
- Telephone

Duty of confidence

A duty of confidence arises when sensitive information is obtained and/or recorded in circumstances where it is reasonable for the subject of the information to expect that the information will be held in confidence. For information to have a quality of confidence it is generally accepted that:

- it is not “trivial” in its nature;
- it is not in the public domain or easily available from another source;
- it has a degree of sensitivity; and
- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example, information shared between a solicitor and client or health practitioner and patient.

However, the right to confidentiality is a qualified right. This means that Genomics England is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.

The Caldicott Report

The original Caldicott Report on the Review of Patient Identifiable Information was published in 1997. It found that the issues of patient confidentiality and the security measures in place across the NHS lacked national consistency and as a result of the Caldicott Review, seven key principles have been provided as a guide for the NHS.

Genomics England is a company wholly owned by the Department of Health as such is bound by the Caldicott Principles.

The Caldicott Principles are:

1. Justify the purpose(s) for using confidential information.
2. Don't use personal confidential data unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

For further information and to review the Caldicott Report see: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf