

What do Clinical Geneticists need to know about Data Protection and Information Governance?

Frances Flinter

Caldicott Guardian

Guy's and St Thomas'
NHS Foundation Trust



Background

- Caldicott review of Patient Identifiable Information (PII) reported in 1997: recommendations regulating the use and transfer of PII within NHS organisations and with non-NHS bodies
- NHS organisations must appoint a Caldicott Guardian
- Data Protection Act (DPA) 1997
- Human Rights Act 1998
- Freedom of Information Act 2000
- NHS Code on Confidentiality 2003

6 Caldicott basic principles

- Justify the purposes for using confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law

Email security: hierarchy

- NHSmail: `firstname.surname@nhs.net`
- N3 network: `firstname.surname@XXX.nhs.uk`
- Others: `name@xxx.ac.uk`
`name@hotmail.co.uk` etc.

Email is only as secure as the weakest link

What this means in practice:

- Remove as much identifiable data as possible e.g. names, initials, DoB when discussing patients outside the immediate medical team
- Anonymise/pseudo-anonymise research/audit data
- Store PID (patient identifiable information) securely: only use encrypted media e.g. iron keys
- Register with the Information Commissioner if you store data at home (better not to)
- Destroy data when it is no longer needed

What should you do?

- Know your responsibilities, and comply
- Don't breach confidentiality
- Don't look at information unless you need to
- Don't share passwords
- Don't take information out of the Trust unless necessary
- Only use secure methods of transferring data
- If it is necessary, protect it
 - On paper – keep it in sight or lock it up
 - On electronic devices – encrypt it
- If you lose it – report it