NHS Information Governance

Guidance note: Security of NHS patient data shared for research purposes

Introduction:

The importance of effective information security has been highlighted in recent months through well publicised data handling failures in a range of different UK organisational settings. The Cabinet Office has completed a review of public sector data handling and has established a comprehensive range of minimum security standards. Consequently, NHS guidance for the protection of patient information has been extended and strengthened in order to respond robustly to these requirements.

Guidance for research bodies

It is essential that everyone who has access to information about NHS patients understands and meets appropriate information security standards. Failure to do so may result in loss or corruption of valuable information, embarrassment to, and loss of confidence in, the bodies involved, and potential damage or distress to the patients whose information is involved.

To help systematically identify and consider security issues in detail it is good practice for organisations to develop and agree with partners an information security policy for the system(s) that will process patient information. An illustrative security policy template document has been developed and is available for this purpose from: www.advisorybodies.doh.gov.uk/piag/securitypolicytemplate.rtf

The security policy should identify how protection will be provided for:

- The core system and its peripheral components used to collect or process data including laptop computers, PDAs and other portable devices;
- The removable media (e.g. CRrom)used to store, transport and archive data;
- The locations where data is processed and stored;
- The means, including email or surface mail, that may be used to share data.

Information is most at risk when it is in transfer. In line with the Cabinet Office requirements for the public sector, David Nicholson NHS CEO has prohibited the transfer of unencrypted person identifiable information on electronic media. All transfers of information to and from NHS bodies should reflect this requirement.

Guidelines on encryption to protect person identifiable and other sensitive information are available at:
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryption.pdf

Guidelines on the transfer of bulk person identifiable information are available at:
https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/GPG%20for%20the%20transfer%20of%20batched%20patient-identifiable%20data.doc

Full details of the NHS approach to information security are set out in Information Security: NHS Code of Practice available at:
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes

Information Security is a component of broader Information Governance. Information Governance standards and guidance are held in an information governance toolkit which may be viewed at: www.igt.connectingforhealth.nhs.uk

Digital Information Policy
Department of Health
3 July 2008