BRITISH JOURNAL OF HOSPITAL MEDICINE
MMC Modernising Medical Careers

MODERNISING MEDICAL CAREERS

IN NEXT MONTH'S MMC SUPPLEMENT

Information governance: a guide for the foundation year doctor

Introduction

Information governance is an important aspect of patient care. All staff, including foundation doctors, must abide by the principles.

The National Programme for Information Technology (NPfIT) was established in October 2002 as a part of the NHS modernization programme. This was introduced by the Department of Health to provide better, faster and safer patient care. The aim is to have:

- A patient's record instantly available to any clinician at any location
- Clinical decision support software
- Electronic appointment booking.

Billions of pounds have been spent on improving capacity and performance, enhancing patients' experiences and helping to realize other NHS priorities. These include:

- Building a lifelong electronic health record service
- Providing an electronic booking service
- Providing an electronic prescription service
- Providing IT infrastructure with sufficient connectivity and broadband capacity to meet future NHS needs (NPfIT, 2004).

There are issues around authentication, consent and confidentiality and, thus, appropriate information governance is required.

Information governance

Information governance ensures necessary safeguards for, and appropriate use of, patient and personal information. It provides guidance and an update to the contractual controls that protect patient, system and employee information.

The aims and objectives of the National Information Governance Board for Health and Social Care include:

- The provision of health and social care should be underpinned by informed consent and personal autonomy
- The right information should be available to the right people at the right time to provide individual care while preserving confidentiality
- Patients and service users have a right to confidentiality
- People's information should be stored and shared in a secure manner
- Those providing care must comply with legislation and their professional guidelines
- Trust and public confidence must be promoted
- Transparency about how people's information is recorded, held and used should be increased
- People's knowledge and understanding of the way in which their information is used within health and social care should be improved
- The efficient delivery of health and social care services, including governance, public health, health promotion, epidemiology, education and research
- Recognition of health and wellbeing promotion and harm prevention as essential components of effective health and social care services.

The Ethics and Confidentiality Committee is accountable to the National Information Governance Board and has delegated powers from the board to undertake responsibilities and advise on ethical issues relating to the processing of health or social care information referred to it by the National Information Governance Board.

Scope of information governance, confidentiality and data protection

Information governance provides a consistent way for employees to deal with the

Miss Deepali Trivedi *is Ophthalmologist, Birmingham and Midland Eye Centre, Sandwell and West Birmingham Hospitals NHS Trust, Birmingham B18 7QH,* **Dr Madhavi Joshi** *is Anaesthetist, Maidstone Hospital, Maidstone, Kent and* **Dr Rachel Hooke** *is Working Time Directive (WTD) Implementation Manager, Airedale NHS Trust, Steeton, Keighley, West Yorkshire*

Correspondence to: Miss D Trivedi

many different information-handling requirements, including the Data Protection Act 1998, the common law duty of confidentiality, the NHS Codes of Practice regarding confidentiality, information security and records management, the NHS Care Record Guarantee for England, the international information security standard: ISO/IEC 27002: 2005 and the Freedom of Information Act 2000.

'THE IG CODE' is a useful acronym to remind staff what is expected of them in their day-to-day work. Each letter stands for a prompt that they should consider:
Think – when using personal information
Handle – information securely
Encrypt – all laptop computers and memory sticks
Information – if it is personal, it is private
Governance – you are accountable for personal information
Confidential – prevent unauthorized disclosure
Overheard – remember: sound travels
Do not – share passwords or smartcard personal identification (PIN) numbers – ever
Everyone – has a legal duty to keep personal information safe and secure.

Principles of information security

The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the NHS, the most sensitive data is patient record information. Salient points are:

- Availability – information must be accessible to authorized users at the required time
- Confidentiality – information must be secured against unauthorized access
- Integrity – information must be safeguarded against unauthorized modification.

Useful websites

Connecting for Health re information governance
www.connectingforhealth.nhs.uk/systemsandservices/infogov

National Information Governance Board
www.nigb.nhs.uk/about/guidance

NHS Information Risk Management
www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/nhsinforiskmgt

Registration Authorities and smartcards
www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards

NHS information risk management

Several measures have been implemented to strengthen controls around information security. Those responsible for managing information risks within the NHS include:

- Senior Information Risk Owner – accountable for managing information risks and incidents, fostering culture for protecting and using data and concerned with the management of all information assets
- Caldicott guardian – an adviser in an organization, providing guidelines for patient confidentiality and management of patient information (Connecting for Health, 2009).

Safety measures

Encryption

Use of encryption to protect personal and sensitive information should be encouraged across the NHS. There should be no transfer of unencrypted person-identifiable data in an electronic format. Any data stored on a PC, laptop computer, mobile telephone or other portable device in a non-secure area should be encrypted.

Registration authorities

Registration authorities are responsible for verifying the identity of health-care professionals and workers who wish to register to use the NHS Care Record Service and other national programmes. It is essential that everyone who will have access to patient information has been through the same rigorous identity checks.

Smartcards

NHS Care Record Service smartcards help control who accesses the NHS Care Record Service and what level of access that they can have. For instance, a receptionist may only see the information needed to process an appointment, not the full clinical record.

Confidentiality: NHS code of practice

Patient information should be kept both physically and electronically secure (Department of Health, 2003).

Manual records should be stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently, inaccessible to members of the public and not left, even for short periods, where they might be looked at by unauthorized people, and able to be securely destroyed, such as by shredding (this is essential).

Regarding electronic records:

- Always log out of any computer system or application when work on it is finished
- Do not reveal passwords to others
- Change passwords at regular intervals to prevent anyone else using them
- Avoid using short passwords
- Always clear the screen of a previous patient's information before seeing another.

Conclusions

Information governance covers the secure and appropriate handling of any type of information, including patients' and personal records. It encompasses various laws and codes of practice. It is an important aspect of patient care. You should exercise due diligence when viewing and processing information of any kind. BJHM

Conflict of interest: Dr R Hooke has worked in both management and medicine. Her views are her own and do not necessarily reflect those of her employer or any other organization that she is associated with.

Connecting for Health (2009) *SIROs and Caldicott Guardians.* Connecting for Health, London (www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap/igaf/roles.pdf accessed 6 August 2010)

Department of Health (2003) *Confidentiality: NHS Code of Practice.* Department of Health, London (www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf accessed 6 August 2010)

National Programme for Information Technology (2004) *National Programme Initiation Document.* NPfIT, London (www.connectingforhealth.nhs.uk/about/governance/docs/nationalprog initiationdoc.pdf accessed 6 August 2010)

KEY POINTS

- Information governance includes information security and appropriate use.
- It applies to foundation doctors, as with other staff.
- It covers electronic and paper records, patient and staff records.
- Always be diligent when handling information that could be accessed by someone unauthorized.