

# Examining confidentiality and information governance

Healthcare organisations must have robust systems in place for managing patient confidentiality. This is not only a legal requirement but also an ethical one, as the integrity of the healthcare system is based on mutual trust between clinician and patient. Here, John Beesley explores organisational guidelines for information governance.

Confidentiality is a crucial aspect of any medical relationship with a patient. All healthcare practitioners have a duty of confidentiality to the patient. The duty is enshrined in civil and employment law as well as in relevant regulatory professional codes of conduct and Department of Health guidance. This duty allows patients to have mutual trust and confidence in the carer/patient relationship. Patients allow healthcare staff to collate personal information related to their treatment, but they do so in confidence with the expectation that such information is kept confidential and privacy is respected. There are occasions when patients may lack the mental capacity to extend their trust or they may be unconscious following an accident, but such circumstances do not diminish the responsibility of the healthcare practitioner from maintaining a duty of confidence.

A duty of confidence occurs when one person discloses information to another in circumstances in which it is reasonable to expect that the information will be kept

'A duty of confidence occurs when information is disclosed in circumstances where it is reasonable to expect that it will be kept confidential'

confidential. Healthcare establishments have a duty to ensure systems are in place to protect patient information and are assured such information is only disclosed with the explicit consent of the patient or where legally justified in the best interests of the public. The patient should always be consulted in the first instance if a disclosure of personal information that may identify the patient is required. It is best practice on admission or during pre-operative assessment to inform the patient of how information may be used to assist in the planning of treatment.

Pre-admission patient information leaflets are a useful resource to explain to the patient that the information they disclose may be recorded to assist the carer with planning their effective treatment. Therefore, on admission, the practitioner admitting the patient should verify that the patient understands this process and documents in the patient's case notes such affirmation. It is important to recognise that patients are aware of the choices available to them in respect of how their information may be used or shared. If a patient refuses to allow their information to be shared, the consequences of the choice should be explained to the patient. The local patient advisory liaison officer in the hospital is often an excellent resource to refer a patient to if they have concerns.

The *Confidentiality NHS Code of Practice* was published by the Department of Health (England) in 2003 and in the same year NHS Scotland published the *NHS Code of Practice on Protecting Patient Confidentiality*. Information governance arrangements should comply with the codes, as they are the

standard of care expected in any healthcare facility. The codes provide a guide to all staff involved with information governance in the NHS and in the independent and voluntary sectors. The code has identified patients' health information and their interests must be protected through a number of measures:

- procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality
- recording patient information accurately and consistently
- keeping patient information private
- keeping patient information physically secure
- disclosing and using information with appropriate care.

## LEGAL CONSIDERATIONS OF CONFIDENTIALITY

The duty of confidentiality is protected by common law and statute law. The common law of confidentiality has been set by legal precedent via case law, which has established individual judgements over time. The key principle outlined in the *Confidentiality NHS Code of Practice* is "that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission". The *Data Protection Act 1998* (DPA) is a statutory Act of Parliament that governs the processing and security of data concerning living individuals. This includes personal records, which may consist of paper, electronic records, film and digital photography. The DPA stipulates that patients have the right to be informed about how information pertaining to them may be used, who will have access to it, and those parties to whom such information may be disclosed. Patients should be advised of the local data controller and how to contact this nominated individual if they have any concerns.

Another statutory act is Article 8 of the *Human Rights Act 1998*, which established a right to "respect for private and family life". In the context of healthcare, there is a duty under the terms of this act to safeguard

the confidentiality of healthcare records. The general rule of confidentiality is to keep patient information private.

Healthcare professionals should always be careful to whom they disclose confidential information. Disclosure in a public place or outside of the workplace may lead to a breach of confidentiality, which not only could lead to disciplinary sanctions but also proceedings by the relevant regulatory professional body, the outcome of which could be loss of registration to practise.

One of the greatest current risks involves the management of electronic patient records. Staff are obliged not to leave portable laptops, medical notes or files in unattended cars or accessible areas where they could be stolen. Staff should not take patient records home unless this can be justified. In which case, all records should be anonymous so patients cannot be identified. Anonymisation includes removal of date of birth, name and address. The fact that information has been anonymised does not remove the duty of confidence.

### ELECTRONIC RECORDS

The Confidentiality NHS Code of Practice outlines best practice for the security of electronic records. For example:

- always log out of any computer system or application when work on it has finished
- never leave a terminal unattended and logged in
- do not share log ins with other people – if other staff have need to access records, then appropriate access should be organised for them
- never reveal passwords to others
- change passwords at regular intervals to prevent anyone else using them
- avoid using short passwords or using names or words that are known to be associated with the individual, such as children's names or the names of pets
- use a password-protected screen saver to prevent casual viewing of patient information by others.

When a patient dies it is debatable whether or not any information relating to the individual remains legally confidential. The *Access to Health Records Act 1990* (AHRA) does permit access to records of a deceased by relatives who wish to pursue a claim arising out of concerns with the patient's death. If the patient has undertaken a formal advance directive forbidding access to healthcare notes then such access is denied. Subject to certain safeguards, the AHRA permits patients to see their own manual health records.

**'One of the greatest current risks to confidentiality involves the management of electronic patient records'**

## 'The common law of confidentiality has been set by legal precedent via case law, which has established individual judgements over time'

In certain circumstances the law recognises that disclosure of confidential information is reasonable when such disclosure is in the best interests of the public. This may include situations where a suspected criminal act is about to occur or has occurred. The healthcare individual disclosing information must be able to justify the reasons for this action. Wherever feasible, the consent of the individual should be obtained. The challenge for the healthcare practitioner making the disclosure concerns the correct assessment of a crime as being serious. Alleged murder, rape or child abuse clearly would be justifiable to report; however, fraud, theft or criminal damage to property may not be justifiable to warrant a disclosure. In such circumstances it is advisable to report concerns to a line manager to ascertain whether or not it is in the public interest for a confidence to be breached. The legal system, including magistrates', sheriffs' and coroners' courts can order a healthcare worker to reveal patient confidential information if it is relevant to the case in question.

### CALDICOTT GUARDIAN

In recent times the security of patient information stored and transmitted electronically had been a major issue of concern in the NHS. In 1997 a committee was established under Dame Fiona Caldicott to review patient identifiable information. Her subsequent report made a series of recommendations with regard to confidentiality that all healthcare organisations should take on board within local information governance. A key recommendation of the 1997 Caldicott report was the establishment of the Caldicott Guardian across the NHS to safeguard access to patient-identifiable information. The Caldicott Guardian is responsible for agreeing and reviewing policies governing the protection of patient-identifiable information. Ideally, the guardian should be at trust or health board level and be a senior professional in the organisation.

The Caldicott principles include:

- justify the purpose
- do not use patient identifiable information unless it is absolutely necessary
- use the minimum necessary patient identifiable information
- access to patient identifiable information should be on a strict need to know basis
- everyone should be aware of their responsibilities
- understand and comply with the law.

When disclosing information, healthcare staff are obliged to take reasonable care and always do so in accordance with local policy. Failure to comply may lead to disciplinary

action. Answering a telephone enquiry about a patient may present a challenge. Staff are required to check the identity of the caller and whether or not the patient has identified the person as a key contact. If the person is not a key contact, such as the next of kin, the caller can be referred to the key contact. Some organisations manage the risk by telephoning the caller back to check they have a legitimate right of access.

An effective information governance strategy includes regular review and audit to ascertain that best practice is being adhered to. The NHSIA Information Governance Toolkit is a useful resource for healthcare establishments. Clear policies should be in existence for confidentiality to be respected. The duty of confidentiality should also be an implied term in contracts of employment, with a breach of confidentiality leading to verbal, written warnings or even dismissal for gross misconduct.

### IGNORANCE IS NO DEFENCE

Healthcare workers have a responsibility to be aware of the principles of the law with regard to the duty of confidentiality. Ignorance of the law is no defence if a breach occurs and the cause of the breach can be attributed to the healthcare worker. Similarly, the healthcare worker should be familiar with the duty of confidentiality as laid out in the respective clauses of their regulatory professional code of conduct. Each and every healthcare worker is accountable for their actions and therefore must be able to justify their actions when a decision is made to disclose confidential patient information. ■

### FURTHER READING

- Department of Health. *Confidentiality NHS Code of Practice*. London: DH, November 2003. [www.ecric.org.uk/nhs\\_conf\\_code.pdf](http://www.ecric.org.uk/nhs_conf_code.pdf).
- Dimond B. Confidentiality. 8: Role of the NHS trust and patient confidentiality. *Br J Nurs* 1999; 8(17): 1175-6.
- General Medical Council. Serious communicable diseases. 1997. [www.gmc-uk.org/guidance/current/library/serious\\_communicable\\_diseases.asp](http://www.gmc-uk.org/guidance/current/library/serious_communicable_diseases.asp).
- NHS Executive. *Caldicott Guardians*. Health Service Circular 1999/012. London: DH, 1999.
- NHS Scotland. *NHS Code of Practice on Protecting Patient Confidentiality*. 2003. [www.confidentiality.scot.nhs.uk/publications/6074NHSCode.pdf](http://www.confidentiality.scot.nhs.uk/publications/6074NHSCode.pdf)

John Beesley LL.M Healthcare Law RGN is an independent healthcare consultant.