*Advances in Psychiatric Treatment (2002), vol. 8, pp. 291–296*

# Confidentiality and security of clinical information in mental health practice

Roy McClelland & Victoria Thomas

*This is the second in a series of papers on health informatics. The first, by Lewis (2002), looked at information organisation and communication. Future papers will consider knowledge management, audit, telemedicine, secondary uses of patient information and working clinical systems.*

'Security holds the key' was the title of a newspaper article concerned with e-commerce (D. Sumner-Smith, *The Sunday Times*, 6 February, 2000, p. 3.13). However, it applies just as readily to the health sector. The need to safeguard the confidentiality of information that patients share with clinicians is as fundamental as the principle of consent. This issue has come to the fore in the context of the rapid developments and applications of information and communication technologies within society in general and within the health sector in particular. There are also changing societal expectations regarding access to information, confidentiality and disclosure. The emerging scenarios present significant challenges in relation to the traditional methods used to deal with the privacy and confidentiality of personal information (Anderson, 1995). In addition to the impact of new technologies, consideration also needs to be given to the impact of changes in health care organisation and practice, for example multi-disciplinary and multi-agency working. Mental health services are in many respects at the vanguard of these changes, where the ideals of community care, shared care and seamless care depend fundamentally on good communication and information sharing. Failures in communicating information, particularly across sectoral boundaries, have led to significant problems in patient care, as revealed in several recent enquiries into homicides (Northamptonshire Health Authority & Northamptonshire Social Services, 1999).

In recent years there have been significant changes in the ways in which the health service values and utilises information about patients, both within the health service itself and across boundaries with other organisations, including non-statutory agencies. While it has always been important to exchange patient information for direct patient care, for the effective operation of the health service and for planning, changes in the way the health service operates have created new demands for information. Within these contexts there is a need to establish a new culture for handling health care information – a culture that recognises, understands and responds to the changing structure of health care and health care delivery systems, which depend increasingly on the ready sharing and manipulation of patient information (France, 1997).

A new and ambitious information strategy for the National Health Service (NHS) has recently been introduced. Its central purpose is to ensure that information is used to help patients receive the best possible care:

> 'A modern and dependable NHS needs accurate and instantly accessible information. This is vital for improving care for patients, for improving the performance of the NHS, and the health of the nation' (NHS Executive, 1998: p. 5).

Roy McClelland is Professor of Mental Health at Queen's University Belfast and a consultant psychiatrist at Belfast City Hospital Trust. He is Chairman of the Irish Association of Suicidology and a trustee for the Centre for Trauma Conflict Transformation, Omagh. He has a longstanding interest in undergraduate and postgraduate education and training. Victoria Thomas worked at the Royal College of Psychiatrists' Research Unit for 5 years as a key member of its clinical practice guidelines development team and its Clinical Governance Support Service. She is now Research and Development Fellow for the National Guidelines and Audit Patient Involvement Unit (College of Health, St Margaret's House, 21 Old Ford Road, London E2 9PL, UK. Tel: 020 8880 7719; fax: 020 8983 1553; e-mail: v.thomas@collegeofhealth.org.uk), an independent unit established to support the involvement of patients and carers in the National Institute for Clinical Excellence's clinical guidelines and audit programmes.

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press

To achieve this purpose the information strategy anticipates lifelong electronic health records for every person in the country, 24-hour access to patient records, seamless care for patients contacting general practitioners, hospitals and community services and fast and convenient public access to information. Inevitably the introduction of information and communication technologies, with the aim of improving the effectiveness and efficiency of health care, brings with it new risks and concerns over the security and confidentiality of patient information.

There is therefore a tension between the needs of patient information to optimise the quality of care and the expectation of patients that information about them will be kept confidential. As the *Report on the Review of Patient-Identifiable Information* (Department of Health, 1997), hereafter referred to as the Caldicott Report, notes, balancing such potential conflicts requires the development of and adherence to explicit and transparent principles of good practice on all aspects of patient-identifiable information.

# Ethical principles and legal framework

While terms such as security, confidentiality and privacy are often used interchangeably there are sufficient differences in their meanings and application to justify brief attention to their definitions (Box 1).

## Ethical principles

Confidentiality considered from a duty perspective is grounded in the principle of respect for autonomy – health professionals explicitly or implicitly promise their patients that they will keep confidential the information provided to them, and keeping promises is a way of respecting autonomy. There are consequentialist arguments supporting keeping a confidence, for without promises of confidentiality patients are far less likely to share the private and sensitive information required for their care. From a professional perspective the requirement of confidentiality appears as early as the Hippocratic Oath and was reaffirmed in the Declaration of Geneva (1948). From a European perspective EC countries are bound by Article 8 of the European Convention on Human Rights, which stipulates 'everyone has the right to respect for his private and family life, his home and his correspondence' and by Article 10 of the Convention on Human Rights and Biomedicine, which states 'everyone has the right to respect for private life in relation to information about his / her health care'.

Nevertheless the duty of confidentiality exists within a wider social context in which other moral obligations may compete. These competing appeals set limits to medical confidentiality and arise from two principal sources. The first is the patient's best interests (the principle of beneficence). The second is public interest (the principle of justice). The new College guidance on confidentiality provides practical advice on decision-making in situations where these ethical principles may conflict with one another (Royal College of Psychiatrists, 2000).

## Legal basis

Confidentiality and privacy are also legal concepts and the relationship between health care professionals and their patients carries legal obligations of confidence as well as moral ones (Box 2).

The Human Rights Act (1998) allows individuals for the first time to pursue claims in UK courts. The European Convention may be invoked in proceedings for established torts such a breach of confidence or to bring an action against a public

**Box 1 Definitions**

*Secrecy* is a state in which information is withheld, whether private or confidential

*Privacy* refers to the condition of limited access to a person and is a much broader concept than limited access to information about a person. Infringement of privacy occurs when unauthorised access is gained to an individual's privacy (Schoeman, 1984)

*Confidentiality* is concerned with keeping secret information given to a person by another person. Infringement of confidentiality occurs when the receiver or holder of that information fails to protect or deliberately discloses that information to someone else without the giver's consent (Beauchamp & Childress, 1994)

*Security* of information is a broader concept than confidentiality, embracing the protection of privacy and confidentiality and also integrity and accuracy. In general it refers to the processes, both technical and organisational, necessary to protect information collection, storage and transmission

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press

**Box 2 Obligations to maintain confidentiality**

*Legal*
Data Protection Act 1998
Human Rights Act 2000

*Clinical governance requirements*
To implement Caldicott recommendations
Common Law

*Professional duty*
General Medical Council confidentiality
Protecting and providing information

authority on the basis of the convention's right to privacy under Article 8. As this Act has only recently come into force we must await the impact of these new rights on existing rules concerning confidentiality. Like common law, it provides for judgements on the balance between the rights of the individual and the needs of society.

Within the UK and Ireland there is a Common Law duty of confidence. Two recent decisions by the European Court of Human Rights have confirmed the applicability of Article 8 of the European Convention to the disclosure of medical information protected by the duty of professional secrecy. The countries of the European Community (EC) are now bound by the requirements of the EC Data Protection Directive (European Parliament & Council of the European Union, 1995), which is the most sweeping recent attempt to protect privacy and in principle gives individuals unprecedented control over information about themselves. Other directives such as 97/66 EC (European Parliament & Council of the European Union, 1997) concerning the processing of personal data and the protection of privacy in the telecommunications sector also have an impact on health care practice. Each member state is required to enact appropriate legislation for the implementation of these initiatives. In Ireland and in England the Data Protection Act recently implemented the requirements of the EC Directive and regulates the data subject's right to privacy. According to Section 55 of the English Act the unlawful obtaining or disclosure of personal data constitutes an offence. Guidance from the Data Protection Commissioner in relation to the requirements of the Act can be found at http://www.dataprotection.gov.uk/dpa98.htm. The statutory requirements of clinical governance include the provision of appropriate safeguards regarding access to and storage of confidential patient information as recommended by the Caldicott Report. It should be noted that Section 60 of the Health and Social Care Act 2001 empowers the Secretary of State to use patient-identifiable information without the consent of patients, where it is deemed necessary for the support of NHS activity (see Secondary uses of patient information below).

In addition to these legal obligations on confidentiality, doctors have a professional duty to maintain confidence, and the misuse of confidential medical information is likely to be regarded as serious professional misconduct (General Medical Council, 2000). Patient information is confidential to that patient and should never be disclosed without consent, unless, exceptionally, it is justified for some lawful purpose.

## Principles for good practice

Two authoritative sources of good practice for the use of patient-identifiable information within the NHS are the Department of Health's (1996) *The Protection and Use of Patient Information* and the recommendations within the Caldicott Report (Department of Health, 1997). The Department of Health guidance defines patient information as 'all personal information about members of the public held in whatever form by or for NHS bodies or staff' (p. 5) and includes non-health information, for example details of domestic circumstances. The guidance states that information may be passed on for a particular purpose with the patient's consent or on a need-to-know basis. The circumstances outlined in the guidance are 'for NHS purposes where the recipient needs the information because he/she is or may be concerned with the patient's care and treatment' (p. 6), and also for a wide range of other purposes (Box 3). There is also a need for patients to be fully informed of the uses to which information about them may be put.

**Box 3 Clinical information-sharing within the National Health Service (NHS)**

*The following may be required*

1 Clinical care
2 Assuring and improving the quality of patient care and treatment
3 Monitoring and protecting public health
4 Coordinating NHS care with that of other agencies
5 Effective health care administration
6 Teaching
7 Statistical analysis and medical or health service research to support 1–5 above
8 Alignment for NHS purposes

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press

**Box 4 Caldicott principles (Department of Health, 1997)**

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised with continuing uses regularly reviewed, by an appropriate guardian

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s)

Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum of identifiable information is transferred or accessible as is necessary for a given function to be carried out

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality

Each use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements

The Department of Health guidance stresses the importance of anonymising personal information wherever possible. The Caldicott Report identifies a number of general principles that should be applied to all flows of patient information (Box 4). The Report recommends that every flow of information, current or proposed, should be tested against these principles. It is noteworthy that the report also recognises that in order to address general concerns regarding patient confidentiality a new culture for handling information is required.

## Security arrangements

Given that clinical responsibility for maintaining confidentiality resides with consultants, we should seek assurances that appropriate policies and protocols are operational within our own trusts. The principles developed for protection of patient information apply whether held on paper, computer systems or other media. While the situation with respect to electronically held information is not in principle different from paper-based information, these new technologies raise new risks and concerns regarding unauthorised or inappropriate access. Threats to security can arise from accidental causes owing to human error or system failure or acts of nature such as fire, or owing to deliberate breaches of security either from within the health care organisation or from external hackers.

The Caldicott Report identifies steps that should be taken to optimise the security and privacy of personal health information (see Box 5). These fall into three groups:

(a) enhancing cultural awareness on issues surrounding confidentiality
(b) developing the organisational framework for access to and use of patient information
(c) developing privacy-enhancing technologies.

Privacy-enhancing technology refers to a range of approaches by which security of data can be improved. The two principal means of enhancing privacy and maintaining the integrity of clinical information are restriction of access and the anonymisation of records. Good security practice includes both sound physical as well as logical access controls. Access to individual paper-based records should only be granted for persons with a direct clinical responsibility to a given patient. For electronically held patient-based information, logical access controls include the use of passwords and 'electronic fingerprinting'.

**Box 5 Approach for enhancing security and confidentiality**

Enhance cultural awareness on issues of confidentiality

Develop organisational frameworks for access to and use of patient information

Develop privacy enhancing technologies

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press

One way of reducing the risk of access to patient-identifiable information is the use of a reference identifier and removing all other identifying information. The NHS number is such a unique personal identifier. While all patients have had a number in the past, a new number has recently been issued and is being widely implemented within the primary and secondary care sectors. This is a 10 digit number in which the 10th digit acts as a check digit, a means of minimising the risk of transposing the other 9 digits. While the use of a coded identifier may enable other patient-identifiable items to be removed, it is essential to prevent unauthorised access to systems that allow relevant patient information to be accessed using this identifier.

Wherever possible, person-based information should be maintained in a non-identifiable form. Encryption is a method for anonymising electronically held patient information. It is the process by which data are converted into a sequence of alternative characters, by applying a set of rules (or key) that both generates the encrypted material and is capable of recreating the original information. NHS policy and procedures for encryption are presently under review and further information and advice can be obtained at http://www.NHSIA.nhs.uk, searching under encryption.

A complementary method for anonymising patient information is the use of separate databases in which clinical information is separated from patient-identifier information. The secondary database retains the non-identifiable patient information, which may be used for a range of purposes.

## *Secondary uses of patient information*

In common with all other areas of health care, patient information is required increasingly for evidence-based practice, a rational approach to service management, and the commissioning and planning of services. This secondary use of patient information raises particular concerns about confidentiality and security. While not qualitatively different from other health information, the sensitivity of information within mental health practice makes this an especially important issue. One of the concerns raised in the Caldicott Report is the variability of practice on such issues as how much patient information is used, what procedures are followed to ensure confidentiality and where responsibilities lie.

Fundamental to the ethical secondary uses of patient information is either patient consent or anonymisation. It has until quite recently been assumed that anonymised patient information and its secondary use within the health service to support, for example planning and research, does not constitute a breach of confidentiality in the absence of patient consent. This position was challenged in a recent court decision where it was held that anonymised use was a breach of confidentiality. However, the Court of Appeal Judgement ruled that as long as a patient's identity was protected, it would not be a breach of confidence to disclose to a third party without the patient's consent (Court of Appeal, 2000).

Reference has been made to Section 60 of the Health and Social Care Act 2001. This Section was introduced as a transitional measure to deal with the present practical constraints of either the consenting process or anonymisation arrangements and to permit patient-identifiable information to be used for essential NHS activities such as health registers and health screening. Given public sensitivities surrounding such arrangements the legislation included the establishment of a patient information advisory group to scrutinise applications for exemption from the usual consenting/anonymisation requirements. To deal with the anticipated large number of requests, for example there are over 250 disease registers, the Department of Health proposes 'class regulations' under Section 60 to enable patient-identifiable information to be used for a number of broad but limited purposes. At the time of writing three classes have been proposed: disease and other registers; communicable disease and other risks to public health; and occupational health and safety.

# Conclusion

The confidentiality, safety and security of patient information is not just a technical issue. Most importantly it relates to organisational culture and structure. As doctors we have responsibility for the confidentiality of patient information and a vested interest therefore in both the culture and the processes, both human and technical, that ensure the security of the information held on our patients.

# References

Anderson, R. (1995) NHS-wide networking and patient confidentiality, *BMJ*, **311**, 5–6.

Beauchamp, T. L. & Childress, J. F. (1994) *Principles of Biomedical Ethics*. Oxford: Oxford University Press.

Court of Appeal (2000) Regina v Department of Health, ex parte Source Informatics Ltd. *Times Law Reports*, 18 January, 17–18.

Department of Health (1996) *The Protection and Use of Patient Information, Guidance from the Department of Health*. London: Department of Health.

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press

—— (1997) *The Caldicott Committee Report on the Review of Patient-Identifiable Information*. London: Department of Health.
—— (2001) *Health and Social Care Act 2001: Consultation Proposals*. Leeds: Department of Health.
European Parliament & Council of the European Union (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal*, **L281**, 31–50.
—— (1997) *Directive 97/66 EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector*. Brussels: European Parliament & Council of the European Union.
France, E. (1997) Data privacy in medicine. A perspective offered by the Data Protection Registrar. *British Journal of Healthcare Computing and Information Management*, **14**, 20–22.
General Medical Council (2000) *Confidentiality: Protecting and Providing Information*. London: GMC.
Lewis, A. (2002) Health informatics: information and communication. *Advances in Psychiatric Treatment*, **8**, 165–171.
NHS Executive (1998) *Information for Health. An Information Strategy for the Modern NHS 1998–2005*. London: NHS Executive.
Northamptonshire Health Authority & Northamptonshire Social Services (1999) *The Independent Inquiry into the Care and Treatment of Wayne Licorish*. Northampton: Northamptonshire Health Authority.
Royal College of Psychiatrists (2000) *Good Psychiatric Practice: Confidentiality*. Council Report CR85. London: Royal College of Psychiatrists.
Schoeman, F. D. (ed) (1984) *Philosophical Dimensions of Privacy: an Anthology*. New York: Cambridge University Press.

## Multiple choice questions

1. Regarding the ethical and legal basis of security and confidentiality:
   a from a duty perspective confidentiality is grounded in the principle of respect for autonomy
   b the declaration of Geneva states an absolute obligation on doctors to maintain confidentiality
   c the European Convention on Human Rights is not legally applicable to medical information
   d the European Convention on Human Rights and Biomedicine states an absolute right to the respect for privacy
   e the Data Protection Acts in Ireland and England have their origins in EC 97/66 concerning the protection of privacy in telecommunication.

2. Regarding security arrangements for patient records:
   a consultants do not have responsibility for maintaining the confidentiality of their patients' records
   b trust arrangements for access to patient information arise as a result of plans to introduce the electronic patient record
   c privacy enhancing techniques are specifically relevant for electronically held information
   d electronic databases of patient information held centrally by the NHS pose particular concerns for security
   e the Caldicott principles apply equally to paper-based and electronically held information.

3. The following are among the general principles identified within the Caldicott Report regarding the confidentiality of patient information:
   a patient-identifiable information items should not be included unless it is essential for the specified purposes of that flow
   b where use of patient-identifiable information is considered essential the consent of the patient's consultant should first be sought
   c only those who need access to patient-identifiable information should have access
   d each use of patient-identifiable information should be lawful
   e in the case of patients who lack capacity each use of patient-identifiable information should be discussed with a parent/guardian as appropriate.

**MCQ answers**

| 1 | 2 | 3 |
|---|---|---|
| **a T** | **a F** | **a T** |
| **b T** | **b F** | **b F** |
| **c F** | **c T** | **c T** |
| **d F** | **d T** | **d T** |
| **e F** | **e T** | **e F** |

https://doi.org/10.1192/apt.8.4.291 Published online by Cambridge University Press