

Patient confidentiality: ethical, legal and regulatory responsibilities

Howard Marsh and John Reynard*

Department of Urology, Medway Maritime Hospital, Gillingham, Kent, and *Department Churchill Hospital, Oxford, UK

Accepted for publication 5 March 2009

INTRODUCTION

Confidentiality is fundamental to the trust upon which the doctor-patient relationship is founded. This is recognized in the Hippocratic oath, the UK NHS Confidentiality Code of Practice [1] and more recently in the NHS Constitution [2]. A duty to respect confidentiality is the subject of clear guidance from the General Medical Council (GMC) [3], whilst the legal obligation to respect confidentiality is determined by case law and enshrined in statute.

Recent high-profile cases of lost data have focused the spotlight on the security of centrally held personal information. Although there have so far been no high-profile cases involving lost medical data, current practices with regard to maintenance and storage of medical records, together with the prospect of a central electronic patient record [4], should encourage every doctor to focus their attention on ways in which they can avoid sensitive information getting into the wrong hands.

In this article we discuss the legal and regulatory framework governing confidentiality; provide a reference source for the extensive literature on the law and regulation of confidentiality; and offer advice on matters of relevance to daily practice, such as the sending of confidential information by e-mail and how one should reconcile conflicting legal and regulatory guidance on, e.g. patient consent to disclosure of a medical report commissioned by a third party.

THE ETHICAL BASIS OF CONFIDENTIALITY

The ethical basis for confidentiality is not a new concept. The Hippocratic Oath states: 'Whatever, in connection with my professional practice... I see or hear in the life

of men, which ought not to be spoke abroad, I will not divulge, as reckoning that all such should be kept secret'. The British Medical Association (BMA) defines confidentiality as 'the principle of keeping secure and secret from others, information given by or about an individual in the course of a professional relationship' [5].

A doctor has a duty to respect patient confidentiality because: (i) Information about a person's health is private; (ii) a patient's willingness to provide information of relevance to diagnosis and treatment is founded on a guarantee of confidentiality.

THE LEGAL BASIS OF CONFIDENTIALITY

The duty to respect confidentiality is governed by common law and statute.

THE COMMON LAW AND CONFIDENTIALITY

Justice Boreham summarized the common law duty to respect confidentiality in *Hunter v Mann* [6]: 'the doctor is under a duty not to disclose, without the consent of his [or her] patient, information which he [or she], the doctor, has gained in his professional capacity, save... in very exceptional circumstances'. (In the case in question, these exceptional circumstances existed. The defendant doctor had been asked for information that might have resulted in the apprehension of a suspect wanted for dangerous driving in a stolen vehicle. The court held that doctor's duty of confidentiality was overridden by the statutory duty imposed by the then Road Traffic Act).

The document 'NHS Information Governance' goes further to say 'in practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must

not normally be disclosed without the consent of the patient' [7].

If a disclosure is made which is not permitted, then under the common law the patient can seek redress in the law, not only against the organization but also *against the individual responsible for the breach*.

STATUTORY OBLIGATIONS TO RESPECT CONFIDENTIALITY

(i) The Data Protection Act 1998: The Act states that all personal data must be 'processed... fairly and lawfully'. 'Processed' means storing the information, disclosing or using it. Processing of such data, without consent, is allowed where it is necessary for medical purposes (treatment, diagnosis, research) and is undertaken by a health professional who has a duty of confidentiality. Thus, the day-to-day sharing of confidential data contained in medical records does not require a patient's consent, for the obvious reason that such a requirement would unnecessarily complicate the process of care.

(ii) The Human Rights Act 1998: Article 8 of The Human Rights Act (the right of respect for private and family life) requires that private information, such as medical notes, is kept private. It is not difficult for a patient to establish that any disclosure of their medical records, without their consent, is *prima facie* a violation of Article 8. However, under Article 8 the right to confidentiality is not absolute. It is qualified by section [2]: 'there shall be no interference by a public authority with the exercise of this right except... in the interests of national security, public safety... for the prevention of crime... or for the protection of the rights and freedoms of others'.

Thus, the interests of the individual patient must be balanced against the public's interests in preventing and solving crime, in

the maintenance of public health, and in freedom of speech (a free press). A patient who argues that their human rights have been violated must overcome the fairly wide interpretation of the law that public bodies are given for justifying disclosure.

THE PROFESSIONAL REGULATION OF CONFIDENTIALITY: GOOD MEDICAL PRACTICE

Whilst legal regulation and ethical obligations with regard to respect for confidentiality are largely in step, it should be remembered that the law sets a *minimum* standard that is not always reflected in the high standards set by, e.g. professional regulatory bodies [1,3].

In 'Good Medical Practice' the GMC gives clear guidance on the professional duties of doctors to protect confidentiality [3]. In many respects these regulatory requirements impose a far more onerous obligation than those laid down in the common law, as a breach of GMC guidance might lead to disciplinary action and the possibility of a finding of serious professional misconduct, for which a doctor can be suspended from the medical register.

NHS GUIDANCE

There is an extensive body of literature detailing the approach that individuals and NHS bodies should take in order to safeguard patient confidentiality (Appendix [7-9]).

COMPULSORY DISCLOSURE – WHEN MUST A DOCTOR DISCLOSE CONFIDENTIAL INFORMATION?

A doctor's duty of confidentiality is not absolute. Other than in response to a court order, the three circumstances in which medical information that is otherwise confidential may be disclosed or shared are:

(i) During the normal process of care. The BMA states 'In the absence of evidence to the contrary, patients are normally considered to have given implied consent for the use of their information by health professionals for the purpose of providing the care they have come to receive' [5] whilst the GMC advises that 'Most people understand and accept that information must be shared within the health care team in order to provide their care' [10].

(ii) In the interests of the public good. The law recognises that there is a balance between the duty to respect the confidentiality of the individual and that required to protect the public interest (usually in terms of preventing or investigating serious crime or harm to a third party [11]). In common law this was established in both *Hunter v Mann* [6] and *W v Edgell* [12]. In the latter case W, a paranoid schizophrenic, had been detained in a secure hospital for shooting and killing five people. Following refusal of his application for release his solicitors commissioned a report from Dr Edgell, an independent psychiatrist. Dr Edgell found that W had a long-standing and continued interest in home-made bombs, and concluded that W remained a threat to the public. Dr Edgell gave the medical director of the secure hospital and the Secretary of State a copy of his report, to facilitate W's continued treatment. W issued a writ against Dr Edgell seeking damages for breach of confidence. His claim was dismissed: 'A consultant psychiatrist who becomes aware, even during the course of a confidential relationship, of information which leads him . . . to fear that [the decision to release W] may be made on the basis of inadequate information and with a real risk of consequent danger to the public is entitled . . . to communicate . . . his concerns to the responsible authorities.' (Lord Bingham, [12]).

The GMC position is that 'Personal information may be disclosed in the public interest, without the patient's consent, and in exceptional cases where patients have withheld consent, where the benefits to an individual or to society of the disclosure outweigh the public and the patient's interest in keeping the information confidential' [10].

(iii) Where a patient consents to disclosure of a medical report commissioned by a third party. Legal and GMC guidance is conflicting. There is no legal requirement to show the patient a copy of the report; the courts regard the fact that the patient commissioned the report (e.g. during their application for life insurance) as evidence that they consent for their insurance company to see the report [13]. The GMC on the other hand imposes a more onerous obligation on doctors, and states that when providing a report to a requesting organization: 'doctors should offer to show patients the report, or give them copies, whether or not this is required by law' [10].

In our opinion doctors would be well advised to follow the more stringent guidelines of the GMC (as this body determines the doctor's fitness to practice) and show the patient a copy of the report *before* it is sent.

CONFIDENTIALITY IN THE CONTEXT OF AUDIT AND RESEARCH

To comply with the Data Protection Act, research using patient data requires either the patient's consent or that the data should be anonymised, so that patients cannot be identified. Where identifiers are required and consent is genuinely not practicable, then an application previously had to be made to the Patient Information Advisory Group. However, as of January 2009 this application has to be made to the new Ethics and Confidentiality Committee of the new National Information Governance Board for Health and Social Care (<http://www.nigb.nhs.uk/ecc>).

Regarding clinical audit, the GMC states [10]: 'Clinical audit is essential to the provision of good care. All doctors in clinical practice have a duty to participate in clinical audit. Where an audit is to be undertaken by the team which provided care, or those working to support them, such as clinical audit staff, you may disclose identifiable information, provided you are satisfied that patients: have been informed that their data may be disclosed for clinical audit, and their right to object to the disclosure; and have not objected'.

A TOPICAL AREA INVOLVING CONFIDENTIALITY – SUMMARY CARE RECORD (SCR)

As part of the NHS National Information Technology Programme, 'Connecting for Health' [14], an online health record is being planned for every person in England – the SCR [4]. This will initially comprise GP records and the intention is that people will have to actively opt out if they do not want to have a SCR [15]. However, it is difficult to opt out if you are not aware of the implementation of the system. This model of consent has been criticised by the BMA [16,17] and was the subject of an independent evaluation by University College London, which concluded 'The "implied consent" model for creating and accessing a person's SCR should be revisited, perhaps in favour of 'consent to view' at the point of access' [18].

COMMON SITES WHERE PATIENT CONFIDENTIALITY MIGHT BE COMPROMISED: INADVERTENT DISCLOSURE

There are several situations where confidentiality can be breached accidentally [11]:

Communication on the ward with colleagues

- Phone consultations – easily overheard by all around you;
- 'Corridor' conversations – breaches of confidentiality have been reported in 11% of lift journeys made by doctors [19];
- Ward rounds in multi-bed bays;
- Student presentations in multi-bed bays.

For example, consider having such conversations or discussions in the doctor's office. There is no easy solution to the difficulty encountered on ward rounds in multi-bed bays, but at least one can pull the curtains around the patient and speak quietly.

Communication with relatives

- This is a common scenario; a relative asks for details of a patient's condition, treatment or prognosis with the assumption that you can divulge this information instantly and without any recourse to the patient. Confidentiality is about protecting privileged information between a patient and you. Third parties (relatives) are not entitled to share in this information unless the patient consents.
- 'He won't be able to cope with the diagnosis': the doctor needs to determine the patient's best interests, not the relatives. Their input is important, but your responsibility with regard to confidentiality is to the patient.
- When a relative telephones you asking for information, you must first seek consent from the patient. In the case of a patient with dementia or who is unable to consent (e.g. the unconscious patient in the Intensive Treatment Unit) the decision whether to divulge confidential information is based on the 'best interests' principle. It will usually be in the patient's best interests to inform relatives of the patient's situation, unless there is good evidence that the patient had expressed a desire that such information should not be disclosed. In these situations it is usual practice to share such information with the relatives.

Computers

- Data entry. The NHS Chief Executive Officer has prohibited the transfer of unencrypted person-identifiable information on electronic media [20]. An NHS encryption tool is now available [21].
- Detailed and comprehensive guidance is available on computer security policies, particularly regarding the use of laptops [22].
- Passwords must be kept secure and changed regularly.
- Logging off – remember to do so, particularly on computers in 'public' places (wards, theatres, clinic rooms). When viewing images on the Picture Archiving and Communications System, remember to log off from the last patient's images before the next patient enters the room.

E-mail communication

- An NHSmail account is the only BMA and Department of Health approved e-mail service for securely exchanging clinical data between NHS staff.
- This means patient identification data and other sensitive information can be safely emailed on this account as long as it is only sent to *another* NHSmail user, and information relating to patients is clearly marked and properly addressed. E-mail outside the NHSmail system might not be secure.

SUMMARY

There is an extensive literature on the legal and regulatory framework governing confidentiality. A common sense approach, together with a working knowledge of the law and regulatory requirements of the NHS and GMC, should protect both the security of sensitive information and doctors from breaches of confidentiality.

CONFLICT OF INTEREST

None declared.

REFERENCES

- 1 DoH. NHS Confidentiality Code of Practice, 2003
- 2 DoH. The NHS Constitution, 2008
- 3 GMC. Good Medical Practice, 2006
- 4 DoH. Connecting for Health: Summary Care Record
- 5 BMA. Confidentiality and disclosure of Health Information, 1999
- 6 Hunter v Mann [1974] QB 767
- 7 DoH. NHS information governance – guidance on legal and professional obligations, 2007
- 8 DoH. Endorsements of the NHS Code of Confidentiality from the Information Commissioner, the GMC and the BMA
- 9 DoH. NHS Security Management Code of Practice, 2007
- 10 GMC. Confidentiality: Protecting and Providing Information, 2004
- 11 Bourke J, Wessely S. Confidentiality. BMJ 2008; 336: 888–91
- 12 W v Edgell [1990]
- 13 Kapadia v London Borough of Lambeth [2000] IRLR 699
- 14 DoH. Connecting for Health
- 15 Kidd MR. Personal electronic health records: MySpace or HealthSpace? BMJ 2008; 336: 1029–30
- 16 BMA. Inquiry into the electronic patient record and its use-response from the British Medical Association, 2007
- 17 Foster M. Patient record study backs doctors' fears on consent. BMA News 2008 (10 May 2008)
- 18 Greenhalgh T, Wood GW, Bratan T, Stramer K, Hinder S. Patients' attitudes to the summary care record and HealthSpace: qualitative study. BMJ 2008; 336: 1290–5
- 19 Vigod SN, Bell CM, Bohnen JM. Privacy of patients' information in hospital lifts: observational study. BMJ 2003; 327: 1024–5
- 20 DoH. NHS Information Governance: Guidance note: Security of NHS patient data shared for research purposes, 2008
- 21 DoH. NHS Encryption Tool, 2008
- 22 DoH. NHS Information Governance: Laptop security policy, 2008

Correspondence: John Reynard, Department of Urology, Churchill Hospital, Oxford, UK
e-mail: john.reynard@orh.nhs.uk

Abbreviations: GMC, General Medical Council; BMA, British Medical Association; SCR, Summary Care Record.

APPENDIX

The NHS Confidentiality Code of Practice (November 2003) [1]:

Establishes working practices to deliver patient confidentiality, as required by law and policy, within all parts of the NHS, by

protecting patient information, informing patients how confidential information is used, providing choice for patients in whether their information can be disclosed or used in particular ways and by improving ways of protecting, informing and providing choice. Endorsed by the Information Commissioner, the GMC, the BMA and the Medical Research Council [8].

Information Security Management: NHS Code of Practice (April 2007) [9].

A 'guide to the methods and required standards of practice in the management of information security' in the NHS. Highlights the responsibility of the *individual*.

NHS Information Governance-Guidance on Legal and Professional Obligations (September 2007) [7].

A clear and succinct introduction to the legal basis of confidentiality and protecting patient information.

The NHS Constitution (June 2008) [2].

Published in June 2008 (marking the 60th anniversary of the foundation of the NHS); sets out the core principles of the NHS in England and Wales; makes several commitments to patients in the form of rights including 'the right to privacy and confidentiality' and 'the right to access your own health records'.