MEDICAL RECORDS

USE AND ABUSE

HEIDI TRANBERG & JEM RASHBASS

FOREWORD BY JOHN PATTISON

CRC Press
Taylor & Francis Group

Medical Records Use and Abuse

Heidi Tranberg

Research Associate
Clinical and Biomedical Computing Unit
University of Cambridge

Jem Rashbass

Director of Clinical and Biomedical Computing
University of Cambridge
Director of the Eastern Cancer Registry
and Information Centre

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First published 2004 by Radcliffe Publishing

Published 2018 by CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

ISBN-13: 978-1-85775-604-3 (pbk)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library.

Typeset by Advance Typesetting Ltd, Oxford

Contents

Foreword

It is always a relief when the information you need to address a problem arrives just in time. So it is with the timely publication of this book. The UK government has embarked on one of the world's most challenging IT projects – The National Programme for Information Technology – which will transform the delivery of healthcare across the National Health Service. Through the programme, patients will have a life-long electronic health record accessible from healthcare centres across the country and ultimately their own homes. The days of lost patient notes, repeated laboratory tests and unknown medication should become a thing of the past.

With these changes will come significant opportunities and challenges for the way we handle medical records. We must ensure that the safeguards are in place to protect patient confidentiality and that when we need to use medical information for purposes not directly related to an individual's own medical care, such as health service planning, performance monitoring and research, it is undertaken in a transparent and appropriate way.

This book provides the background and practical guide for all those of us who face these challenges. Written by a lawyer and a clinical informatician, it provides the fusion between the legal issues and the practical clinical ones. There are clear explanations of the current legal framework of the Data Protection and Freedom of Information Acts and the effects of Section 60 of the Health and Social Care Bill. These are set in the context of real-world applications; for example, there is guidance for those who need to develop consent forms for research or respond to requests from the public for healthcare information and there is extensive coverage of the rights of the patient who wishes to access their own records.

Several of the more complex issues that have a significant impact on policy are also dealt with in depth. A chapter is devoted to the complexities of anonymising data, how this might be implemented, the benefits that can be achieved and challenges arising from pseudonymisation. There is information for those involved in medical research and what they must do to guarantee that patients' rights are protected when they request or use clinical information. The background to 'consent' and the impact that implied and explicit consent can have on the way records are collected and used is particularly well covered.

This book has many audiences, all of whom will gain from the easily accessible information within it. Caldicott guardians, research ethics committee

members, and all those researchers and clinicians who need to analyse patient information will have a particular need for this handbook. Patients and the public should use it to understand how their healthcare information is protected and used. Its arrival could not have come at a better time.

Sir John Pattison
Former Director of Research, Analysis and Information
Department of Health
March 2004

About the authors

Heidi Tranberg trained in both law and psychology, and worked for a number of years as a solicitor in a leading Australian law firm, specialising in intellectual property, information technology, biotechnology and privacy. During this time she played a key role in developing the firm's health privacy website. Since joining the Clinical and Biomedical Computer Unit at Cambridge University, Heidi has been involved in a variety of projects, including research of health privacy issues, strategic planning and marketing activities, and the development of an electronic dyslexia-screening test. She has published several papers and articles on legal and ethical issues.

Dr Jem Rashbass has a background in medicine, molecular biology and pathology. Since 1997 he has been Director of the Clinical and Biomedical Computing Unit at Cambridge University, a group responsible for developing novel computer applications in clinical teaching, practice and medical research. He is also the Director of the Eastern Cancer Intelligence Centre – providing cancer registration and analysis across the east of England, he holds an honorary consultant contract in histopathology at Addenbrooke's NHS Trust and is a Non-executive Director of the NHS Information Authority.

Acknowledgements

The authors greatly appreciate the assistance of a number of experts who generously shared their views and experiences on various issues discussed in the book. In particular, they would like to thank Professor Don Detmer and Baroness Onora O'Neill, both of the University of Cambridge; Marlene Winfield, Head of Patient and Citizen Relations at the NHS Information Authority; and Janine Brooks, a Caldicott Guardian at the NHS Information Authority.

Chapter 1

Introduction

Protecting the privacy of patient information is a major challenge facing the health sector. Today's patients expect, and are entitled by law to receive, a high standard of medical privacy. Given the complexity and function of the health system, however, it can be difficult to meet this expectation.

Healthcare is an information-rich activity, in that it involves the collection, use and disclosure of large quantities of sensitive personal data. Such information is not only required by health professionals directly involved in patient treatment, but also the many groups who indirectly contribute to the delivery of quality healthcare. Administrators, policy makers, researchers, educators, public health bodies and auditors are just some of the groups that require access to patient data to ensure that high quality, cost-effective medical treatment is delivered in a timely and appropriate manner. Making this information available, without compromising patients' rights, is a complex task.

How have health privacy rights evolved?

The right to personal privacy is not a new concept. It has been recognised for many years, and was even included in the 1948 United Nations Universal Declaration of Human Rights.[1] Initially, however, the right to privacy was more concerned with protecting people from unwanted intrusions into their personal lives, rather than inappropriate disclosures of their personal data.

As information came to play a larger role in society, this focus began to shift. The increased use of computers in the 1970s and 1980s brought new opportunities to store and analyse large volumes of data, and prompted interest in individuals' right to control the use and dissemination of their personal information, a right often referred to as 'informational privacy'.[2] In light of the circumstances that caused this type of privacy to be recognised, in the UK protection was originally limited to data that

were stored electronically.* As many medical records still were stored in paper files, this development had only a limited effect on patient data privacy.

In many countries, various disease- or condition-specific privacy acts also provided some assurance of privacy,** although these acts had only a fairly limited impact on the overall level of protection of patient data. This was partly because the special protection was only extended to information relating to a limited number of conditions, usually those considered particularly sensitive or potentially damaging to a patient's reputation, such as mental illness or sexually transmitted disease. In many cases, protecting patients' privacy was also not the sole, or even major, concern of these disease-specific acts, with mandatory reporting obligations often being imposed in addition to restrictions on disclosure.† The protection provided by disease-specific privacy legislation, therefore, was limited and piecemeal, and did little to recognise patients' rights to informational privacy.

For many medical records the greatest source of privacy protection continued to be doctors' general duty of confidentiality. This duty prevents doctors from using or disclosing confidential information obtained within the confines of the doctor–patient relationship for any purpose other than that for which it was provided. In theory, the duty of confidentiality should prevent medical information obtained for the purpose of treating a patient from being used for any secondary purpose without the patient's permission. In practice, however, it did not always provide such a comprehensive level of protection. This was caused in part by a tendency to interpret the obligation in accordance with the paternalistic approach to medicine that prevailed at the time, which often resulted in patients' rights or wishes taking second place to doctors' professional judgement.[3] It was standard practice in most institutions to use medical records for a range of secondary purposes, such as audit, research and administrative activities, without consent – either on the assumption that consent was not required (as the use posed little risk to patients) or that it could be implied from patients' actions. In any event, it was often very difficult for patients to monitor the way in which their medical records were used, as they did not usually have a right to verify

* The Data Protection Act 1984 Section 1 defines 'data' as 'information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose'.

** For example, in the UK, identifying information about a patient who is being treated for venereal disease may not be disclosed other than to a medical practitioner in connection with the patient's treatment or to prevent the spread of the disease (NHS (Venereal Disease) Regulations 1974 and NHS Trusts (Venereal Diseases) Directions 1991).

† In the UK, for example, there is a mandatory requirement for any practitioner who performs an abortion to notify the Chief Medical Officer. The same legislation then goes on to restrict the extent to which the information contained in such a notice can be disclosed. (Abortion Act 1967 Section 2 and Abortion Regulations 1991 Sections 4 and 5.)

what had been recorded about them or how it had been disclosed; often, there was not even a record of the disclosures that had been made.*

This situation has changed substantially in the last decade. Information privacy is now recognised to a greater extent than ever before – a development principally led by international initiatives. Following the adoption of data protection agreements by the Council of Europe[4] and the Organisation for Economic Co-operation and Development (OECD)[5] in the 1980s, in 1995 the European Community developed a new binding Directive setting out a number of data protection principles.[6] The Directive required signatory countries to establish national legislation implementing its terms. In the UK, this was achieved by the enactment of the Data Protection Act 1998, which came into effect on 1 March 2000. As the Directive imposed restrictions on the transfer of personal data to countries that did not have equivalent data protection regimes, it also prompted change outside the EU.

Today, most European and other industrialised countries have established, or are moving toward, comprehensive data protection legislation.[7] Although there are a number of differences, both minor and significant, between the specific legislation adopted in each country, the general approach tends to be quite similar. Most countries have established a single regime for protecting all types of personal data, whether financial, educational, social or otherwise, with only minor concessions given to the greater sensitivity of some types of data, such as that pertaining to health. The exception to this trend is the US, where medical information is protected by specific federal legislation.**

Since the 1995 EC Directive, further international agreements governing the privacy of health information have been signed.† In the UK, however, the most significant restriction on the way information is collected and managed continues to be the Data Protection Act 1998 and the various policies and guidelines that seek to implement its terms.

* This is because medical records are usually considered to be the property of the health provider, not the patient. Under the common law, doctors are only required to grant patients access to their medical record if doing so is necessary to fulfil the doctor's duty to act in the patient's best interest (R v Mid Glamorgan Family Health Services Authority (1995) 1 All ER 356).

** Health Insurance Portability and Accountability Act 1996. However, this legislation only applies to a limited number of entities that could potentially control health information, namely health plans, healthcare providers that electronically transmit healthcare information, and healthcare clearing houses. For information controlled by other types of organisations, the level of protection will depend upon the applicable state law.

† Under the 1997 Council of Europe's Convention on Human Rights and Biomedicine, for example, a new right 'not to be informed about health information' was included in the concept of 'respect for private life and the right to information'.

What information is recorded about patients?

Medical records are an important and comprehensive source of information about all aspects of an individual's health. Traditionally, however, particularly in primary care, medical records were relatively brief documents, used mainly to refresh the doctor's memory.[8] Very detailed information was not required as doctors tended to be well-acquainted with patients and their families, often knowing more about their patients' medical histories than the patients themselves. In recent years, however, the nature of medical records has changed substantially.

First, there has been a significant increase in the amount and type of information included in medical records. Advances in medical knowledge and diagnostic techniques have enabled doctors to uncover much more information about individuals' health status, all of which must be documented. In some cases, these developments have made it possible for entirely new types of information, such as genetic data, to be collected. It has also become common practice for doctors to record more non-medical information about patients, such as lifestyle choices and family history, in response to the increasing evidence of the effects of such factors on health.

There has also been a change in the manner in which information is recorded, with greater emphasis being placed on more complete, detailed and consistent documentation. This largely is attributable to the increase in the number of people involved in the care of patients, both over their lifetime and during a single care episode, which has arisen from the increased specialisation of the medical profession, the delivery of care through medical teams, and the greater mobility of society.[9] (Estimates in the US suggest that 150 people will look at a patient's medical record during a stay in hospital.)[10] As a result, the primary role of medical records is no longer that of a memory aid, but a vital communication tool, needed to share detailed and varied information amongst a potentially wide range of health professionals. In addition, the increased risk of legal challenge brought about by the growing number of medical negligence claims has prompted doctors to document their findings and decisions more fully. For example, it is now standard practice for significant, negative, clinical results to be recorded explicitly, rather than to assume that they are negative by omission.

In addition to these changes there has also been an increase in the use of medical records for secondary purposes not directly connected with the provision of care.[9] Doctors are now only one of the many groups of people with legitimate interests in accessing this important source of data. Identifiable patient information is used routinely for the purpose of clinical and financial audits, health service planning, resource management, authenticating health providers' payment claims and patients' health

insurance claims, rehabilitation and social welfare programmes, and education and training. Information from medical records is also used extensively in epidemiological and health service research, and for the purpose of disease monitoring. With the rise in personal injury, child custody and other types of litigation, it has also become increasingly common for medical records to be accessed via compulsory court processes.[11] Added to this is the growing number of new users of health information, such as medical and surgical suppliers and pharmaceutical and information technology companies.[8]

Although the protection of medical records may not be a new issue, therefore, changes in the health industry have altered its nature and importance.

Why protect the privacy of health information?

The primary reason for respecting the privacy of health information is to protect patients from the negative effects brought about by the loss of personal privacy. Medical records contain intimate and sensitive information, which, if inappropriately used or shared, could embarrass or distress patients, and even cause them financial or other damage (*see* p. 23). Fearing the unwanted exposure of personal information, patients may also avoid medical treatment or withhold facts from their doctor, both of which could have serious health consequences.[12]

In many cases, however, using or disclosing medical information poses little, if any, risk to patients. Providing that basic security procedures are followed, such as anonymising identifiable data and storing data securely, the use of patients' information for research, audit or planning purposes is unlikely to cause them damage or distress, and may even provide some indirect benefit.[13] This does not mean that providing this protection ceases to be important, as there are still persuasive moral and ethical arguments for respecting informational privacy.

It is claimed, for example, that there is a strong connection between protecting the privacy of personal information, and the concept of personal autonomy.[9,12,14] Protecting privacy tends to increase individuals' confidence in their ability to control and manage the direction of their lives, a development that sits well with the modern view of healthcare as being centred on the rights of the patient. Many patients place a high value on the privacy of their personal information, in particular that relating to health, with the right to control how it is used often considered as fundamental as the right to make decisions about their private behaviour. Giving patients control over their personal information demonstrates an understanding and respect for

their status as an autonomous and free-thinking patient, which is likely to increase their satisfaction with the health system and their belief in its ability to provide a high quality service.

These arguments capture the emotional and human components of privacy and explain the importance of ensuring it is protected, but they do not address the more difficult issue of how this protection should be achieved.

How should health information be protected?

Numerous studies, reports and debates have investigated the best way of protecting patient information. From these, several basic principles have emerged. It is generally accepted, for example, that patients should be kept informed of, and given some control over, the way in which their information is used, and that data should only be disclosed on a 'need to know' basis.[15] Attempts to formulate the specific policies and rules needed to implement these principles, however, have revealed a significant divergence in views. Devising general principles (it seems) is much easier than agreeing on specific requirements.

This problem is well illustrated by the diversity of opinion concerning the circumstances in which individuals' rights to privacy should be overridden. Most people, be they patients, healthcare providers or policy makers, agree that there must be some limits on individuals' right to control the way their information is used. To maintain a safe and functional society, and to protect the well-being of those living within it, it is essential that certain groups are given access to some types of information, irrespective of patients' wishes. Apprehending and prosecuting criminals, providing emergency medical treatment and maintaining population disease registers are just three vital activities that would be jeopardised if access to information was always dependent upon individuals' agreement.

Accepting that there should be exceptions to the requirements of the Data Protection Act 1998, however, is not the same as agreeing upon the nature of those exceptions. Does the possibility of a medical breakthrough, for example, justify research being carried out on patient data without patients' permission? Would the situation be different depending upon the importance of the condition being investigated and the researcher's confidence of finding a cure? Equally, does the need to prevent and detect crimes justify the disclosure of patients' information in all circumstances, or only in relation to particularly serious offences, in which case, how is 'seriousness' measured? No matter how necessary or important an exception may be,

determining its exact nature and scope will always be a matter of some contention.

Differences of opinion have also arisen in relation to the programmes and policies needed to deal with other aspects of medical record privacy. There is much uncertainty, for example, as to the best way to inform patients of the way in which their information is used and to obtain their consent for this (*see* Chapter 3). There is also disagreement over the level of anonymity of data that is needed to protect patients' identities, and the control, if any, that patients should have over this type of information (*see* Chapter 10).

Much of the difficulty in obtaining consensus arises from the large number and variety of people who will be affected by the rules and policies that are ultimately implemented. Nearly everyone is involved in the health system as a patient, a professional, or both, and their experiences vary considerably. The different views of clinicians, researchers, medical bodies, privacy advocates and patient groups reflect their different interests in accessing (or preventing access to) information, and the way in which increased privacy will assist or hamper their aims. Even patients with different healthcare experiences have divergent views.[16] More often than not, groups that seek extended rights to access personal information, such as administrators and researchers, do so for very worthy purposes, whereas those advocating increased privacy protection also have valid reasons or concerns.

To ensure that the rules can apply widely, the privacy requirements in many healthcare directives and guidelines have been drafted in fairly general terms. For example, the government's new plan for information-sharing in the public services promises to give citizens a choice over how their personal information is used, 'wherever possible'.[17] Although this avoids controversy in the short term, and gives the government considerable flexibility when implementing the rules in the future, it does little to clarify the rules that will apply. Whether this provides an acceptable level of privacy protection depends entirely upon the government's interpretation of what is 'possible'.

The Data Protection Act 1998

The Data Protection Act 1998 regulates the collection, use and disclosure of information that relates to identifiable individuals (called 'personal data'). It does this by establishing eight privacy rules – known as the 'data protection principles' – with which anyone controlling personal data (called 'data controllers') must comply. Among other things, these principles provide

that information must only be collected and used fairly, lawfully and for one of the purposes, or in compliance with one of the conditions, set out in the Act.* In practice, this often means that data controllers have to obtain individuals' consent if they wish to collect or use any data about them.

Data controllers are also required to give individuals basic information, at the time of collection, about who will use the data and the purpose or purposes for which it will be used.** They cannot subsequently use that data in any manner incompatible with those purposes (the second data protection principle). The Act also imposes restrictions on the amount of information collected (the third data protection principle) and the manner in which it is stored (the seventh data protection principle), and grants individuals certain rights in respect of their information, including the right to verify what has been recorded about them and how it has been used.† The data protection principles are considered in further detail in Box 1.1 and a flowchart summarising the main decisions to be made before using potentially personal data is provided in Figure 1.1 (*see* page 10).

Box 1.1

Data Protection Act 1998: glossary and the data protection principles

The Data Protection Act 1998 requires all data controllers to comply with the data protection principles when processing personal data. Key terms used in the Act include:

- *Data* – information recorded or stored, either electronically or in a relevant filing system (a set of information about individuals that is structured so that information about a particular individual is readily accessible). This definition would cover much of the information held by healthcare providers, including medical records, appointment books and staff files.
- *Personal data* – data from which a living person can be identified. This covers both data that identify a person (such as a medical record containing a patient's name), as well as data that identify a person when read in conjunction with other information which is likely to be available to the person accessing it. The NHS Number is classified as personal data, therefore, despite the fact that it does not reveal a patient's identity, as the information needed to identify the patient can be obtained relatively easily through the NHS Tracing Service.

* First data protection principle. The purposes and conditions are listed in the Data Protection Act 1998, Sections 2 and 3.
** Data Protection Act 1998, paragraphs 2 and 3, Schedule 1, Part 2.
† Data Protection Act 1998, Section 7.

- *Data controller* – the person or organisation that determines the purpose for which, or manner in which, personal data will be processed. There may be more than one data controller for a single item of personal data.
- *Data subject* – the individual who is the subject of the personal data. A data subject must be a living person, but need not be a UK citizen.
- *Processing* – collecting, recording, holding, altering, using, disclosing, transmitting, erasing or destroying data.

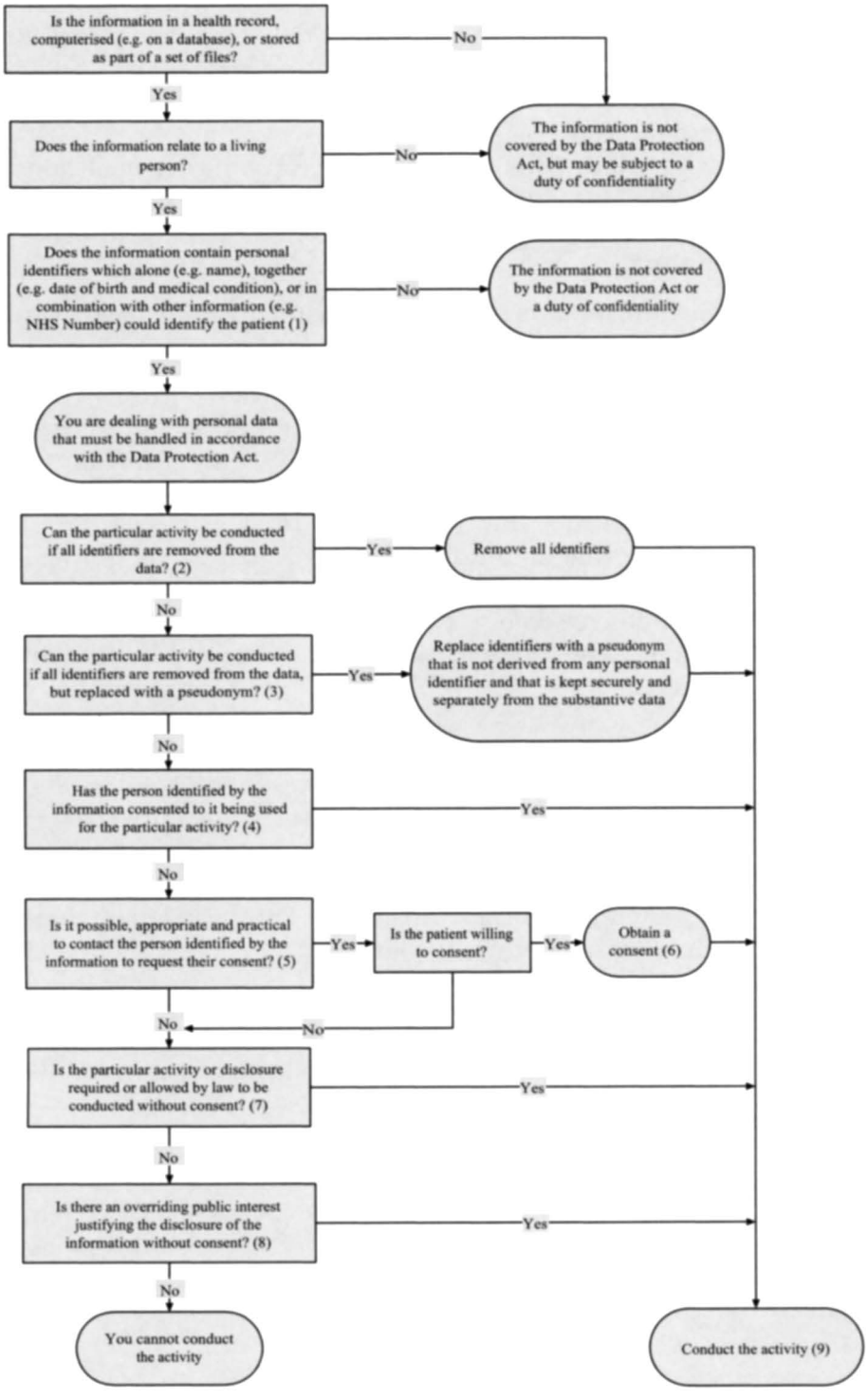
In a simplified form, the data protection principles require that personal data:

1 are processed fairly and lawfully
2 are only processed for one or more specified and lawful purposes; data cannot be used or disclosed for any purpose incompatible with the specified purposes for which it was collected, without the permission of the data subject
3 are adequate, relevant and not excessive for the purpose for which they are required
4 are accurate and up to date
5 are not kept any longer than is necessary for the purpose for which they are required
6 are processed in accordance with the rights of the data subject under the Data Protection Act 1998. These include: the right to access any personal data held about them; to prevent processing of data that is likely to cause them damage or distress; and to prevent processing for the purpose of direct marketing
7 are protected from unauthorised or unlawful processing or loss
8 are not transferred to countries outside the European Union that do not have adequate data protection laws.

For healthcare providers, the first and second of these principles will usually be the most important. These are discussed in greater detail in Chapter 3, *see* Box 3.1.

The Data Protection Act gives some concession to the private and intimate nature of health information by including it in a special class of personal data, known as sensitive data, to which more stringent conditions apply.* When collecting sensitive data, for example, data controllers must, in addition to the usual obligations, satisfy one of a number of extra conditions

* Data Protection Act 1998, Section 2.


Is the information in a health record, computerised (e.g. on a database), or stored as part of a set of files?
No
Yes
Does the information relate to a living person?
No
The information is not covered by the Data Protection Act, but may be subject to a duty of confidentiality
Yes
Does the information contain personal identifiers which alone (e.g. name), together (e.g. date of birth and medical condition), or in combination with other information (e.g. NHS Number) could identify the patient (1)
No
The information is not covered by the Data Protection Act or a duty of confidentiality
Yes
You are dealing with personal data that must be handled in accordance with the Data Protection Act.
Can the particular activity be conducted if all identifiers are removed from the data? (2)
Yes
Remove all identifiers
No
Can the particular activity be conducted if all identifiers are removed from the data, but replaced with a pseudonym? (3)
Yes
Replace identifiers with a pseudonym that is not derived from any personal identifier and that is kept securely and separately from the substantive data
No
Has the person identified by the information consented to it being used for the particular activity? (4)
Yes
No
Is it possible, appropriate and practical to contact the person identified by the information to request their consent? (5)
Yes
Is the patient willing to consent?
Yes
Obtain a consent (6)
No
No
Is the particular activity or disclosure required or allowed by law to be conducted without consent? (7)
Yes
No
Is there an overriding public interest justifying the disclosure of the information without consent? (8)
Yes
No
You cannot conduct the activity
Conduct the activity (9)

set out in the Act.* For the most part, however, the same privacy regime applies to all types of personal data.

The Data Protection Act has been criticised on a number of grounds.[18] Many commentators argue that it is inappropriate for dealing with the particular considerations relevant to health information, it having been written principally for the financial and commercial sectors. Relying on consent as the main means of controlling the use that can be made of personal information, it is suggested, is not the optimum method for addressing privacy concerns in the health sector, as patients often lack the knowledge, experience, understanding or confidence to determine how their health information should be used.[19] A number of the requirements of the Act are also quite uncertain or ambiguous, making it difficult for healthcare providers and those advising them to implement appropriate privacy policies.[20] For example, while it is clear that anonymous data are not covered by the data protection requirements, the Data Protection Act 1998 does not clarify

---

Figure 1.1 (opposite): The 1998 Data Protection Act. The flowchart summarises the main decisions that need to be made before using or disclosing information. The issues are presented in a simplified form to provide a general overview of the topic. The flowchart is not intended to provide a full summary of, or a comprehensive guide to, the Data Protection Act. Key: 1 = *see* Chapter 10, in particular p. 132; 2 = the Caldicott Committee definition of an identifier, *see* Chapter 10, p. 131. Examples include names, addresses, telephone numbers, email addresses, date of birth, NHS numbers, local hospital codes, bank account details and employers' or family members' names or contact details; 3 = *see* Chapter 10, pp 132–4; 4 = *see* Chapter 3, p. 32. Consent can be express or implied, although for some activities or disclosures (such as those that are likely to be controversial or to affect patients directly) it may be better to obtain express consent (*see* Chapter 3, p. 33 and pp 36–8). The activity must also be covered by the scope of the consent (*see* Chapter 3, p. 34); 5 = relevant considerations include: the cost, time and effort required to contact each patient (affected by the numbers of patients and the age and currency of the records); the likelihood that contacting the patients wil be distressing for patients and their families; the likelihood that a significant number of patients may have died; 6 = *see* 4 above; 7 = legislation that may allow or require the disclosure of identifiable health information includes the Abortion Act 1967, the Terrorism Act 2000 and the regulations made under the Health and Social Care Act 2001 (Section 60), *see* Chapter 7, pp 95–6 and Chapter 8, pp 110–11. The disclosure of patient information may also be required under the terms of a witness summons or other court order (*see* Chapter 9, p. 117); 8 = *see* Chapter 8; 9 = it will be necessary to comply with additional requirements set out in other legislation or other relevant ethical guidelines. For example, in the case of research, ethics review board approval will be required.

*The additional conditions are contained in the Data Protection Act 1998, Schedule 3.

what standard of anonymity needs to be met. Despite relying quite heavily on the concept of individual consent, it also fails to give any guidance about the type of consent required and how specific it should be.

Added to these concerns is the continuing controversy over the many exceptions and exemptions that enable data controllers and government bodies to avoid the data protection requirements. Although most of the exceptions actually contained in the Act only arise in relatively specific circumstances, more recent legislation has given the government additional powers to avoid the requirements of the Act.* Many people fear that despite the government's assurances to the contrary, this power will be used too extensively (*see* Chapter 7, p. 96).

In the healthcare sector, problems with compliance further challenge the effectiveness of the Data Protection Act 1998. Despite the Act having been in force for a number of years, the National Health Service (NHS) is yet to modify its practices to comply fully with the new requirements. According to the Information Commissioner, who oversees the administration of the Act, the NHS frequently breaches the legislation by using identifiable patient information without patients' knowledge or consent.[15] This practice, it is suggested, results from an overriding belief within the NHS that the sharing of information benefits many, harms few and is essential for efficiency and expediency.[15] This belief is reinforced by the low regard given to information management within the NHS, as well as a lack of informatics training in the health sector generally. The effect of this is a poor understanding of, and commitment to, the management of patient information.[21]

There is also some uncertainty under the Data Protection Act 1998 with regard to the ownership of personal data. Although the issue of data ownership is relatively straightforward where medical records are created and stored locally, the idea of a national electronic health record, which is part of the government's current proposals, makes this much more complex. If information is collected and entered into the system by patients' general practitioners, but is then stored at the primary care trust level, who is the relevant owner? Does ownership change as data are collated, aggregated and analysed? The Data Protection Act avoids this issue by imposing obligations on 'data controllers', being those who can determine the purpose and manner in which data are used, rather than 'data owners'. However, as a single piece of information can be controlled by a number of different data controllers, there is likely to be much confusion and conflict about privacy and data management responsibilities.

These problems show that, although the Data Protection Act is a key consideration in the issue of medical record privacy, it does not, on its own,

* Health and Social Care Act 2001, Section 60.

provide a complete solution to the existing confusion and disagreement. Of equal importance is the way in which the courts and ethical bodies interpret the Act, the specific policies and plans that are developed to deal with the data protection requirements, and the extent to which these are implemented and enforced. A key component of this is the government's proposed changes to the NHS.

The government's proposal

As part of the government's plan to modernise the NHS, it has developed a new strategy, known as 'Information for Health', which deals with data protection and other information management issues within the NHS.[21, 22] The strategy, which runs from 1998 until 2005, aims to redesign the NHS around the patient.

Under the new plan, information is recognised as a vital factor in the delivery of healthcare, with the ability to provide quality patient care said to be dependent on 'the availability of good information, accessible when and where it is needed'. Without this, a health system is said to be 'at best inefficient and frustrating and at worst dangerous'.[23] The plan therefore aims to improve the way the NHS uses data, and increase data-sharing both within the NHS and with other government organisations.

At the same time, the government also recognises the sensitivity of the information involved in healthcare. It therefore plans to achieve this increased data-sharing in a way that ensures privacy is enhanced, not derogated. Individual deliverables, such as introducing life-long electronic health records, establishing 24-hour online access to patients' records and providing seamless care through the sharing of information between general practitioners, hospitals and community care providers, must all be met without damaging patients' privacy expectations. It remains to be seen whether this will be achieved.

Summary

- Interest in protecting the privacy of personal data, including health data, has increased in recent years.
- More information is collected about patients today than ever before.
- There is relatively high agreement on the general principles that should govern the protection of medical data, but it is much harder to agree on the specific rules and policies.
- The Data Protection Act 1998 is a key consideration but does not provide a complete solution to the problem of medical record privacy.

References

1 United Nations (1948) *Universal Declaration of Human Rights*, Article 12. Adopted and proclaimed by General Assembly resolution no. 217 A (III), 10 December.

2 Health Privacy Working Group (1999) *Best Principles for Health Privacy*. Institute for Health Care Research and Policy, Health Privacy Project, Georgetown University. (www.healthprivacy.org/usr_doc/33807.pdf). (Accessed 24 August 2003.)

3 Coulter A (1999) Paternalism or partnership. *British Medical Journal*. **319**: 719.

4 Council of Europe (1981) Convention for the Protection of Individuals with Regard to the Automatic Processing of Data.

5 Organisation for Economic Co-operation and Development (OECD) (1980) *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*. OECD, France.

6 EC Directive 95/46/EC (1995) On the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 October.

7 Cushman F and Detmer D (1998) Information policy for the US health sector: engineering, political economy and ethics. *Milbank Quarterly Special Edition Electronic Article*, January. (www.milbank.org/art). (Accessed 5 September 2003.)

8 Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure, National Research Council (1997) *For the Record: protecting electronic health information*. National Academy Press, Washington DC.

9 Institute of Medicine (1994) *Health Data in the Information Age*. National Academy Press, Washington DC.

10 George S (2002) Medical privacy and medical research. *CLA-GAB Newsletter of the Cancer and Leukaemia Group B*. **11**: 2.

11 Lowrence W (1997) *Privacy and Health Research (A Report to the US Secretary of Health and Human Services)*, May. (http://aspe.hhs.gov/datacncl/PHR.htm). (Accessed 16 June 2003.)

12 Wynia M, Coughlin S, Alpert S *et al.* (2001) Shared expectations for the protection of identifiable health care information. *Journal of General Internal Medicine*. **16**: 100.

13 Lawlor D and Stone T (2001) Public health and data protection: an inevitable collision or potential for a meeting of minds? *International Journal of Epidemiology*. **30**: 1221.

14 Institute of Medicine (2000) *Protecting Data Privacy in Health Services Research*. National Academy Press, Washington DC.

15 Department of Health (DoH) (2001) *Building the Information Core: protecting and using confidential patient information – a strategy for the NHS*. (www.doh.gov.uk/ipu/confiden/strategyv7.pdf). (Accessed 10 June 2003.)

16 NHS Information Authority, The Consumers' Association, Health Which? (2002) *Share with Care – people's views on consent and confidentiality of patient information*. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

17 Performance and Innovation Unit (2002) *Privacy and Data Sharing: the way forward for public services*. April: 5. (www.number-10.gov.uk/su/privacy/index.htm). (Accessed 10 April 2003.)

18 Knoppers B (2000) Appendix D – Confidentiality of health information: international comparative approaches. In: Institute of Medicine, *Protecting Data Privacy in Health Services Research*. National Academy Press, Washington DC.

19 Starr P (1999) Privacy and access to information: striking the right balance in healthcare. In: *Massachusetts Health Data Consortium, 4th Annual Meeting*, Boston, MA, 16 April. (www.nchica.org/HIPAAResources/Samples/privacylessons/P-101%20Massachusetts%20Health%20Data%20Consortium.htm). (Accessed 13 September 2003.)

20 Strobl J, Cave E and Walley T (2000) Data protection legislation: interpretation and barriers to research. *British Medical Journal*. **321**: 890.

21 NHS Information Authority (1998) *Information for Health*. (www.nhsia.nhs.uk/def/pages/info4health/contents.asp). (Accessed 10 June 2003.)

22 Department of Health (DoH) (2001) *Building the Information Core: implementing The NHS Plan*. (www.doh.gov.uk/ipu/strategy/overview/overview.pdf). (Accessed 10 June 2003.)

23 NHS Information Authority (2002) *Caring for Information – model for the future*, para 1.3. (www.nhsia.nhs.uk/confidentiality/pages/consultation/docs/caring_model.pdf). (Accessed 8 July 2003.)

References

1 Introduction

1 United Nations (1948) Universal Declaration of Human Rights, Article 12. Adopted and proclaimed by General Assembly resolution no. 217 A (III), 10 December.

2 Health Privacy Working Group (1999) Best Principles for Health Privacy. Institute for Health Care Research and Policy, Health Privacy Project, Georgetown University, (www.healthprivacy.org/usr_doc/33807.pdf). (Accessed 24 August 2003.)

3 Coulter A (1999) Paternalism or partnership. British Medical Journal 319: 719.

4 Council of Europe (1981) Convention for the Protection of Individuals with Regard to the Automatic Processing of Data.

5 Organisation for Economic Co-operation and Development (OECD) (1980) Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data. OECD, France.

6 EC Directive 95/46/EC (1995) On the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 October.

7 Cushm an F and Detmer D (1998) Information policy for the US health sector: engineering, political economy and ethics. Milbank Quarterly Special Edition Electronic Article, January, (www.milbank.org/art). (Accessed 5 September 2003.)

8 Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure, National Research Council (1997) For the Record: protecting electronic health information. National Academy Press, Washington DC.

9 Institute of Medicine (1994) Health Data in the Information Age. National Academy Press, Washington DC.

10 George S (2002) Medical privacy and medical research. CLA-GAB Newsletter of the Cancer and Leukaemia Group B. 11: 2.

11 Lowrence W (1997) Privacy and Health Research (A Report to the US Secretary of Health and Human Services), May.

(http: //aspe.hhs.gov/datacncl/ PHR.htm). (Accessed 16 June 2003.)

12 Wynia M, Coughlin S, Alpert S et al. (2001) Shared expectations for the protection of identifiable health care information. Journal of General Internal Medicine. 16: 100.

13 Lawlor D and Stone T (2001) Public health and data protection: an inevitable collision or potential for a meeting of minds? International Journal of Epidemiology. 30:1221.

14 Institute of Medicine (2000) Protecting Data Privacy in Health Services Research. National Academy Press, Washington DC.

15 Department of Health (DoH) (2001) Building the Information Core: protecting and using confidential patient information a strategy for the NHS. (www.doh.gov.uk/ ipu/confiden/strategyv7.pdf). (Accessed 10 June 2003.)

16 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

17 Performance and Innovation Unit (2002) Privacy and Data Sharing: the way forward for public services. April: 5. (www.number-10.gov.uk/su/privacy/index.htm). (Accessed 10 April 2003.)

18 Knoppers B (2000) Appendix D Confidentiality of health information: inter national comparative approaches. In: Institute of Medicine, Protecting Data Privacy in Health Services Research. National Academy Press, Washington DC.

19 Starr P (1999) Privacy and access to information: striking the right balance in healthcare. In: Massachusetts Health Data Consortium, 4th Annual Meeting, Boston, MA, 16 April. (www.nchica.org/HIPAAResources/Samples/privacylessons/P-101%20Massachusetts%20Health%20Data%20Consortium.htm). (Accessed 13 September 2003.)

20 Strobl J, Cave E and Walley T (2000) Data protection legislation: interpretation and barriers to research. British Medical Journal. 321: 890.

21 NHS Information Authority (1998) Information for Health, (www.nhsia.nhs.uk/ def/pages/info4health/contents.asp). (Accessed 10 June 2003.)

22 Department of Health (DoH) (2001) Building the Information Core: implementing The NHS Plan, (www.doh.gov.uk/ipu/strategy/overview/overview.pdf). (Accessed 10 June 2003.)

23 NHS Information Authority (2002) Caring for Information model for the future, para 1.3. (www.nhsia.nhs.uk/confidentiality/pages/consultation/docs/caring_model.pdf). (Accessed 8 July 2003.)

Ref erences

1 Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure, National Research Council (1997) For the Record: protecting electronic health information. National Academy Press, Washington DC.

2 Linowes D (1997) A Research Survey of Privacy in the Workplace. Unpublished White Paper, available from the University of Illinois at Urbana-Champaign.

3 (2003) Medical records found on memory stick. E-Health Insider. 12 March. (www.e-health-media.com/news/item/cfm?ID=383). (Accessed 7 July 2003.)

4 (1995) Hospital clerk's child allegedly told patients that they had AIDS. Washington Post. 1 March: A17.

5 Ernst and Young (2001) The Health Industry and Privacy, (www.ey.com/global/ Content.nsf/ Australia / AABS_-_TSRS_-_The_Health_Industry_and_Privac y). (Accessed 30 May 2003.)

6 Wahlberg D (1999) Patient records on web 2 months. Ann Arbor News. 11 February.

7 Lavelle M (1994) Health plan debate turning to privacy: some call for safeguards on medical disclosure. Is a federal law necessary? National Law Journal. 30 May: 1.

8 Needham K (2003) Watchdog barking over privacy lapses. Sydney Morning Herald. 7 January.

9 Australian Privacy Commissioner (1995) Community Attitudes to Privacy, Infor mation Paper No. 3. Human Rights and Equal Opportunities Commission, Sydney.

10 Office of the Information Commissioner (2001) Annual Report. Office of the Information Commissioner, Sydney.

11 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

12 Health Privacy Project (1999) Exposed: a health privacy primer for consumers. Institute for Health Care Research and Policy, Georgetown University. (www.healthprivacy.org/usr_doc/33806/pdf). (Accessed 10 March 2003.)

13 California Health Care Foundation (1999) Americans Worry About the Privacy of their Computerised Medical Records. (www.chcf.org/press/view.cfm?itemID= 12267). (Accessed 10 March 2003.)

14 Performance and Innovation Unit (2002) Privacy and Data Sharing: the way forward for public services, (www.number-10.gov.uk/su/privacy/index.htm). (Accessed 30 October 2003.)

15 Chester M (2000) Patients' expectations and experiences (ACHCEW contri bution). In: Privacy in the Electronic NHS. (Debate organised by the British Medical Informatics Society, London, 30 November 2000.) (www.bmis.org/privacy2000/chester.doc). (Accessed 10 April 2003.)

16 National Committee on Vital and Health Statistics (1997) Health Privacy and Confidentiality Recommendations, (www.ncvhs.hhs.gov/privrecs.htm). (Accessed 10 April 2003.)

17 The Caldicott Committee (1997) Report on the Review of Patient-identifiable Information. NHS Executive, (www.doh.gov.uk/ipu/confiden/report/index. htm). (Accessed 5 August 2003.)

18 Cambridge Health Informatics Limited (2001) Gaining Patient Consent to Dis closure. (www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf). (Accessed 13 March 2003.)

19 Institute of Medicine (1994) Health Data in the Information Age. National Academy Press, Washington DC.

20 Goldman J and Choy A (2002) Privacy and Confidentiality in Health Research. The Online Ethics Center for Engineering and Science, Case Western Reserve University, (http://onlineethics.org/reseth/nbac/hgoldman.html#f3). (Accessed 30 May 2003.)

21 Department of Health (DoH) (2000) The NHS Plan, (www.doh.gov.uk/nhsplan/ index.htm). (Accessed 15 March 2003.)

22 Medical Research Council (2000) Personal Information in Medical Research. (Updated January 2003.) (www.mrc.ac.uk/pdf-pimr.pdf).

23 Cushman F and Detmer D (1998) Information policy for the US health sector: engineering, political economy and ethics. Milbank Quarterly Special Edition Electronic Article, January, (www.milbank.org/art). (Accessed 5 September 2003.)

24 Detmer D (2000) Your privacy or your health will medical privacy legislation stop quality health care? International Journal for Quality in Health Care. 12:1.

25 Hawker A (2001) Privacy as an Investment. Security, Legal Issues and Confiden tiality Special Interest Group, Birmingham Business School, (www.bham.ac.uk/business/health/cbaOl.htm). (Accessed 15 April 2003.)

26 California Health Care Foundation (1999) Medical Privacy and Confidentiality Survey, (www.chcf.org/documents/ihealth/survey.pdf). (Accessed 10 March 2003.)

Ref erences

1 General Medical Council (2000) Confidentiality: protecting and providing infor mation. GMC, London.

2 NHS Information Authority (2002) Caring for Information model for the future.

3 Department of Health (DoH) (2002) Confidentiality: a code of practice for NHS staff (draft),

4 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

5 Cambridge Health Informatics Limited (2001) Gaining Patient Consent to Dis closure. (www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf). (Accessed 13 March 2003.)

6 Information Commissioner (1998) Data Protection Act 1998: legal guidance. Version 1. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Legal Guid ance'. (Accessed 30 March 2003.)

7 Information Commissioner (2002) Use and Disclosure of Health Data. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Compliance Advice'. (Accessed 10 May 2003.)

8 Department of Health (DoH) (2002) Legal and Policy Constraints on Electronic Records: options, (www.nhsia.nhs.uk/erdip/pages/evaluation/docs/

9 Confidentiality and Security Advisory Group for Scotland (2002) Protecting Patient Confidentiality final report. Scottish Executive Health Department. (www.show.scot.nhs.uk/sehd/publications/ppcr/ppcr.pdf). (Accessed 6 August 2003.)

10 Organisation for Economic Co-operation and Development (OECD) (2000) Literacy in the Age of Information, (wwwl .oecd.org/publications.e-book/ 8100051e.pdf). (Accessed 10 May 2003.)

11 NHS Information Authority (2002) Tees ERDIP Demonstrator Programme, Project 3 consent and confidentiality,

(www.nhsia.nhs.uk/erdip/pages/evaluation/ docs/polsprotreports/teesfinalc&s.pdf). (Accessed 8 July 2003.)

12 NHS Information Authority (2002) ERDIP EHR Issues and Lessons Learned Report.

13 Thombury J (2001) Walsall Natural Community Patient Consent Policy. NHS Information Authority, paras 4.1 and 4.2. (www.nhsia.nhs.uk/erdip/pages/ demonstrator/ wals/ walsall_(12).pdf). (Accessed 8 July 2003.)

14 Department of Health (DoH) (2001) Good Practice in Consent Implementation Guide: consent to examination or treatment, (www.doh.gov.uk/consent/ implementationguide.pdf). (Accessed 5 June 2003.)

15 British Medical Association (1999) Confidentiality and Disclosure of Health Infor mation. BMA, London.

16 Starr P (1999) Privacy and access to information: striking the right balance in healthcare. In: Massachusetts Health Data Consortium, 4th Annual Meeting, Boston, MA, 16 April. (www .nchica. or g / HIP AAResources / Samples / privacy lessons / P-101%20Massachusetts%20Health%20Data%20Consortium.htm). (Accessed 13 September 2003.)

1 Wanless D (2002) Securing our Future: taking a long-term view. HM Treasury.

2 Benson T (2002) Why general practitioners use computers and hospital doctors do not Part 1: incentives. British Medical Journal. 325:1086.

3 Department of Health (DoH) (2002) Delivering 21st Century IT Support for the NHS national strategic programme, (www.doh.gov.uk/ipu/whatnew/deliveringit/ nhsitimpplan.pdf). (Accessed 11 September 2003.)

4 (2003) Poor IT placing patients at risk junior doctors warned. E-Health Insider. 14 May. (www.e-health-media.com/news/item.cfm?ID=426&searchString= information%20system). (Accessed 18 September 2003.)

5 Roscoe T (undated) Paper vs Electronic Medical Records. The Wisdom Centre. (www.shef.ac.uk/uni/projects/wrp/paper.html). (Accessed 30 September 2003.)

6 Schoenberg R and Safran C (2000) Internet based repository of medical resources that retains patient confidentiality. British Medical Journal. 321:1199.

7 Blendon R, Schoen C, DesRoches C, Osborn R and Zapert K (2003) Common concerns amid diverse systems: health care experiences in five countries. Health Affairs. 22:106.

8 (2001) US alliance to promote electronic medical records. E-Health Insider. 14 December. (www.e-health-media.com/news/item.cfm?ID-72&search String=pri vacy). (Accessed 18 September 2003.)

9 NHS Information Authority (1998) Information for Health: para 2.71. (www.nhsia.nhs.uk/def/pages/info4health/contents.asp). (Accessed 10 June 2003.)

10 Health Privacy Working Group (1999) Best Principles for Health Privacy. Institute for Health Care Research and Policy, Health Privacy Project, Georgetown University, (www.healthprivacy.org/usr_doc /33807.pdf). (Accessed 24 August 2003.)

11 Mitchell E and Sullivan F (2001) A descriptive feast but an evaluative famine: systemic review of published

articles on primary care computing during 1980- 97. British Medical Journal. 322: 279.

12 American Health Information Management Association (undated) Confidentiality of Medical Records: a situation analysis and AHIMA's position, (www.ahima.org/infocenter/current/white_paper.cfm). (Accessed 19 September 2003.)

13 Neame R and Kluge E (1999) Computerisation and health care: some worries behind the promise. British Medical Journal. 319:1295.

14 Chin T (2001) Security breach: hacker gets medical records. American Medical News. 29 January. (www.ama-assn.org/amednews/2Q01/01/29/tesaQ129.htm). (Accessed 15 June 2003.)

15 Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure, National Research Council (1997) For the Record: protecting electronic health information. National Academy Press, Washington DC.

16 Mandl K, Szolovits P and Kohane I (2001) Public standards and patients' control: how to keep electronic medical records accessible but private. British Medical Journal 322: 283.

17 Denley I and Smith S (1999) Privacy in clinical information systems in secondary care. British Medical Journal. 318:1328.

18 Anderson R (1996) Security in Clinical Information Systems. University of Cambridge, (www.ftp.cl.cam.ac.uk/ftp/users/rja14/policyll.pdf). (Accessed 11 March 2003.)

19 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

5 Should different medical information be treated differently?

1 Cushman F and Detmer D (1998) Information policy for the US health sector: engineering, political economy and ethics. Milbank Quarterly Special Edition Electronic Article, January, (www.milbank.org/art). (Accessed 5 September 2003.)

2 Performance and Innovation Unit (2002) Privacy and Data Sharing: the way forward for public services, (www.number-10.gov.uk/su/privacy/index.htm). (Accessed 30 October 2003.)

3 NHS Information Authority (2002) Caring for Information model for the future. (www.nhsia.nhs.uk/confidentiality/pages/consultation/docs/caring_model.pdf). (Accessed 8 July 2003.)

4 Kunitz and Associates Inc (1995) Final Report of the Task Force on the Privacy of Private Sector Records. US Department of Health and Human Services, (http://aspe.hhs.gov/pic/pdf/5879.pdf). (Accessed 30 September 2003.)

5 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

6 Markwel D (2001) Commentary: open approaches to electronic patient records. British Medical Journal. 322: 287.

7 British Medical Association (1999) Confidentiality and Disclosure of Health Information. BMA, London.

8 Anderson R (1996) Security in Clinical Information Systems. University of Cambridge, (www.ftp.cl.cam.ac.uk/ftp/users/rja14/policyll.pdf). (Accessed 11 March 2003.)

9 Crosbie D (2000) Protection of Genetic Information: an international comparison. Human Genetics Commission, (www.hgc.gov.uk/business_publications_intemational_regulations.pdf). (Accessed 4 November 2003.)

10 Benkendorf J, Reutenauer J, Hughs C et al. (1997) Patients' attitude about autonomy and confidentiality in

genetic testing for breast-ovarian cancer susceptibility. American Journal of Medical Genetics. 73: 296-303.

11 Weijer C (2000) Family duty is more important than rights. Contribution to ethical debate 'Results of genetic testing: when confidentiality conflicts with a duty to warn relatives'. British Medical Journal. 321: 1464.

12 van der Wouden J and van Amerongen H (2000) View from Dutch general practice. Contribution to ethical debate 'Results of genetic testing: when confidentiality conflicts with a duty to warn relatives'. British Medical Journal. 321: 1464.

13 Leung W (2000) Case study. Contribution to ethical debate 'Results of genetic testing: when confidentiality conflicts with a duty to warn relatives'. British Medical Journal. 321:1464.

6 Accessing your own record

Ref erences

1 Bergen L (1988) Patient access to medical records: a review of the literature. AMR Journal. 18: 102.

2 Cornwall A (1996) Whose Health Records ? Attitudes to consumer access to their health records and the need for law reform. Public Interest Advocacy Centre, Sydney.

3 Office of the Data Protection Commissioner (2001) Subject Access and Health Records. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Compliance Advice'. (Accessed 30 March 2003.)

4 Office of the Information Commissioner (2000) FAQs subject access. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Compliance Advice'. (Accessed 30 March 2003.)

5 British Medical Association (2002) Access to Health Records by Patients. BMA, London.

6 Information Commissioner (1998) Data Protection Act 1998: legal guidance. Version 1. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Legal Guid ance'. (Accessed 30 March 2003.)

7 Department of Health (DoH) (2003) Guidance for Access to Health Records Requests under the Data Protection Act 1998. (www.doh.gov.uk/ipu/ahr/dpal998.pdf). (Accessed 15 June 2003.)

8 Wynia M, Coughlin S, Alpert S et ah (2001) Shared expectations for the protection of identifiable health care information. Journal of General Internal Medicine. 16: 100.

9 NHS Information Authority and Oxford Health Authority (2001) The Develop ment of Patients' Access to Their Online Electronic Patient Record.

10 Jain N (2002) The Bury Knowle EHR Project. Journal of the Torex User Group. 48: 26.

11 UK News (2002) Medical records a review of December 2002 medico-legal news. Medical Litigation Online, (www.medneg.com/news/news.cfm?month= December&year=2002). (Accessed 20 October 2003.)

12 Duncan N (1996) On the record. Australian Medicine. 7:13.

13 Pyper C, Amery J, Watson M, Crook C and Thomas B (2001) Patients' access to their online electronic health records. Paper presented at the Primary Health Care Specialist Group of the British Computing Society Annual Conference, Cambridge, September.

14 NHS Modernisation Agency (undated) Developing Patient-held Records. (www.modern.nhs.uk/serviceimprovement/1338/4668/CHDCReportCover.pdf). (Accessed 13 June 2003.)

15 O'Connor K (1993) Information privacy issues in health care and administration. Paper presented at the Inaugural National Health Informatics Conference, Brisbane, August.

16 Sampford K (1999) Access to Medical Record, Research Bulletin 6/99. Queensland Parliamentary Library. (www.parliament.qld.gov.au/Parlib/Publications_pdfs/books/rb0699ks.pdf). (Accessed 13 June 2003.)

17 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care-people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

18 NHS Information Authority (1998) Information for Health, (www.nhsia.nhs.uk/ def/ pages/info4health/contents.asp). (Accessed 10 June 2003.)

7 Research

1 Lawlor D and Stone T (2001) Public health and data protection: an inevitable collision or potential for a meeting of minds? International Journal of Epidemiology. 30:1221.

2 Goldman J and Choy A (2002) Privacy and Confidentiality in Health Research. The Online Ethics Center for Engineering and Science, Case Western Reserve University, (http://0nlineethics.0rg/reseth/nbac/hg0ldman.html#f3). (Accessed 30 May 2003.)

3 Canadian Institutes of Health Research (2001) Case Studies Involving Secondary Use of Personal Information in Research (Draft).

4 Institute of Medicine (2000) Protecting Data Privacy in Health Services Research. National Academy Press, Washington DC.

5 Al-Shahi R and Warlow C (2000) Using patient-identifiable data for observational research and audit. British Medical Journal. 321:1031.

6 Medical Research Council (2000) Personal Information in Medical Research. (Updated January 2003.) (www.mrc.ac.uk/pdf-pimr.pdf).

7 Cassell J and Young A (2002) Why we should not seek individual consent for participation in health services research. Journal of Medical Ethics. 28: 313.

8 Lowrance W (2002) Learning from Experience privacy and the secondary use of data in health research. The Nuffield Trust, London.

9 Strobl J, Cave E and Walley T (2000) Data protection legislation: interpretation and barriers to research. British Medical Journal. 321: 890.

10 Doll R and Peto R (2001) Rights involve responsibilities for patients, letter to the editor. British Medical Journal. 322: 730.

11 Tondel M and Axelon O (1999) Concerns about privacy in research may be exaggerated. British Medical Journal. 319: 706.

13 Cambridge Health Informatics Limited (2001) Gaining

Patient Consent to Disclos ure.
(www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf).
(Accessed 13 March 2003.)

14 Detmer D (2000) Your privacy or your health will
medical privacy legislation stop quality health care?
International Journal for Quality in Health Care. 12:1.

15 Woolf S, Rothemich S, Johnson R and Marsland D (2000)
Selection bias from requiring patients to give consent to
examine data for health services research. Arch Pam Pract.
9:1111.

16 Roberts L and Wilson S (2002) Argument for consent may
invalidate research and stigmatise certain patient groups,
letter to the editor. British Medical Journal. 322: 858.

17 Verity C and Nicoll A (2002) Consent, confidentiality,
and the threat to public health surveillance. British
Medical Journal. 234:1210.

18 Department of Health (DoH) (2002) Confidentiality: a
code of practice for NHS staff (draft),

19 Anderson R (1998) Information Technology in Medical
Practice: safety and privacy lessons from the United
Kingdom. University of Cambridge, Cambridge.

20 Davies S (2001) Taking Liberties in Confidence: a report
for the Nuffield Trust on the implications of Section 67
of the Health and Social Care Bill, (http: //is.lse.ac.uk/
privacy/healthconfidentiality.doc). (Accessed 23 June
2003.)

21 Information Commissioner (2002) Use and Disclosure of
Health Data. (www.dataprotection.gov.uk/dpr/dpdoc.nsf),
under 'Compliance Advice'. (Accessed 10 May 2003.)

22 General Medical Council (2000) Confidentiality:
protecting and providing infor mation. GMC, London.

23 General Medical Council (2002) Research: the role and
responsibility of doctors. GMC, London.

24 Lowrence W (1997) Privacy and Health Research (A Report
to the US Secretary of Health and Human Services), May.
(http: / / aspe.hhs.gov/ datacncl/ PHR.htm). (Accessed 16
June 2003.)

25 Information Commissioner (1998) Data Protection Act

1998: legal guidance. Version 1. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Legal Guid ance'. (Accessed 30 March 2003.)

26 Department of Health (DoH) (undated) Proposal to Revise Regulations made under Section 60 of the Health and Social Care Act 2001. (www.doh.gov.uk/ipu/act/nhs_databases_consultation_paper.pdf). (Accessed 10 November 2003.)

27 Anderson R (2001) Undermining data privacy in health information. British Medical Journal 322: 442.

28 McCarthy K (2001) Health industry warns of 'sinister' government legisla tion. The Register, 13 March, (www.theregister.co.uk/content/7/17567.html). (Accessed 6 May 2003.)

29 Dyer C (2001) Bill gives government power to breach patient confidentiality. British Medical Journal 322: 256.

30 Anderson R, Hanka R and Hassey A (2001) Clause 67, Medical Research and Privacy: the options for the NHS. (www.cl.cam.ac.uk/ftp/users/rja!4/ hcbillc67.pdf). (Accessed 25 June 2003.)

31 Paterson I (2001) Consent to cancer registration an unnecessary burden. British Medical Journal. 322: 1130.

32 Burnett S, Woof C and Yudkin J (1992) Developing a district diabetic register. British Medical Journal 305: 627.

33 Medicines and Healthcare Products Regulatory Agency (2002) The Yellow Card Scheme: protecting patient confidentiality. (www.mca.gov.uk). (Accessed 21 October 2003.)

34 Brown P (2002) Health bodies defend their right to access patient data. British Medical Journal 324:1236.

8 Public interest

1 General Medical Council (2000) Confidentiality: protecting and providing infor mation. GMC, London.

2 British Medical Association (1999) Confidentiality and Disclosure of Health Infor mation. BMA, London.

3 General Medical Council (2002) Research: the role and responsibility of doctors. GMC, London.

4 Department of Health (DoH) (2002) Confidentiality: a code of practice for NHS staff (draft),

5 Cozens C and Milmo D (2002) Campbell privacy case thrown out. Guardian Unlimited, 14 October, (http://media.guardian.co.uk/presspublishing/story/0,7495,811789,00.html). (Accessed 3 June 2003.)

6 (2003) In brief Naomi Campbell case appeal. Guardian Unlimited, 28 February. (www.guardian.co.uk/uk_news/story/0/3604/904468/00.html). (Accessed 3 June 2003.)

7 Cambridge Health Informatics Limited (2001) Gaining Patient Consent to Disclos ure. (www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf). (Accessed 13 March 2003.)

8 Department of Health (DoH) (2001) Building the Information Core: protecting and using confidential patient information a strategy for the NHS. (www.doh.gov.uk/ ipu/confiden/strategyv7.pdf). (Accessed 10 June 2003.)

9 Brown P (2000) Cancer registries fear imminent collapse. British Medical Journal. 321: 854.

10 The Family Violence Prevention Fund (2002) National Consensus Guidelines on Identifying and Responding to Domestic Violence Victimization in Health Care Settings, (h ttp ://endabuse.org/programs/healthcare/files/Consensus.pdf). (Accessed 3 June 2003.)

11 Cottingham R (2001) Proposals for community violence prevention are naive. British Medical Journal. 322: 677.

12 Department of Health (undated) Proposal to Revise Regulations made under Section 60 of the Health and Social

Care Act 2001. (www.doh.gov.uk/ipu/act/nhs_databases_consultation_paper.pdf). (Accessed 10 November 2003.)

13 General Medical Council (1997) Serious Communicable Diseases. GMC, London.

14 British Medical Association (1996) Interim Firearms Guidance Note. BMA, London.

9 Legal proceedings - a threat to medical record privacy?

1 Woman Abuse Response Program (2003) Reasonable Doubt: the use of health records in legal cases of violence against women in relationships. British Columbia's Women's Hospital and Health Centre, (www.bcifv.org/resources/reasonabledoubt. html). (Accessed 19 May 2003.)

2 Temkin J (2001) Comments in Response to the Criminal Courts Review by the Right Honourable Lord Justice Auld. The Lord Chancellor's Department. (www.lcd.gov.uk/criminal/auldcom /ar/ar5.htm). (Accessed 20 May 2003.)

3 Halsbury's Laws of England Medicine, Pharmacy, Drugs and Medicinal Products, paragraph 18.

4 Halsbury's Laws of England Evidence, paragraph 409.

5 National Legal Research Group (1995) Discovery of a Party's Mental Health Records in Child Custody Matters. Divorce Research Centre, (www.divorcesource.com/ research/dl/childcustody/95oct219.shtml). (Accessed 20 May 2003.)

6 British Medical Association (1999) Confidentiality and Disclosure of Health Infor mation. BMA, London.

7 Winick B (1996) The psychotherapist-patient privilege: a therapeutic jurispru dence view. U Miami L Rev. 50: 249.

8 Sc rutiny of Acts and Regulations Committee (1996) Review of the Evidence Act 1958 (Vic) and Review of the Role and Appointment of Public Notaries. Parliament of Victoria.

9 Shuman D and Weiner M (1984) Privilege a comparative study. Journal of Psychiatry and Law. 12: 373.

10 Beck J (1982) When the patient threatens violence an empirical study of the clinical practice after Tarasoff. Bull Am Acad Psychiatry & Law. 10:189.

11 McNicol S (1992) Law of Privilege. Law Book Company, Sydney: 395.

12 Planned Parenthood of Greater Iowa (2002) Planned Parenthood's Medical Privacy Case Dismissed, (www.ppgi.org/includes/media/proct3102.htm). (Accessed 20

October 2003.)

13 Rothstein M (1997) Preventing the Discovery of Plaintiff Genetic Profiles by Defend ants Seeking to Limit Damages in Personal Injury Litigation. Indiana University. (http://law.indiana.edu/ilj/v71/no4/rothstei.html). (Accessed 19 May 2003.)

10 Anonymous information

1 The Caldicott Committee (1997) Report on the Review of Patient-identifiable Information. NHS Executive, (www.doh.gov.uk/confiden/crep.html). (Accessed 5 August 2003.)

2 Lowrance W (2002) Learning from Experience privacy and the secondary use of data in health research. The Nuffield Trust, London.

3 Information Policy Unit (2002) Options for the Pseudonymisation of Patient Iden tifiable Information (Draft) Version 1.1. Department of Health, London.

4 Goldman J and Choy A (2002) Privacy and Confidentiality in Health Research. The Online Ethics Center for Engineering and Science, Case Western Reserve University, (http://0nlineethics.0rg/reseth/nbac/hg0ldman.html#f3). (Accessed 30 May 2003.)

5 NHS Information Authority (2002) Caring for Information model for the future.

6 Information Commissioner (2002) Use and Disclosure of Health Data. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Compliance Advice'. (Accessed 10 May 2003.)

7 General Medical Council (2000) Confidentiality: protecting and providing infor mation. GMC, London.

8 Department of Health (DoH) (2001) Building the Information Core: protecting and using confidential information a strategy for the NHS. (www.doh.gov.uk/ipu/confiden/strategyv7.pdf). (Accessed 10 June 2003.)

9 Davies S (2001) Taking Liberties in Confidence, a Report for the Nuffield Trust on the Implications of Clause 67 of the Health and Social Care Bill, (http: //is.lse.ac.uk/privacy/healthconfidentiality.doc). (Accessed 23 June 2003.)

10 Information Policy Unit (2003) Draft NHS Number Policy Statement Vol.5, HRDG 025/2003. Department of Health, London, (www.doh.gov.uk/ipu/ahr/ hrdg2503.pdf). (Accessed 21 July 2003.)

11 Cambridge Health Informatics Limited (2001) Gaining Patient Consent to Dis closure. (www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf).

(Accessed 13 March 2003.)

12 Chester M (2000) Patients' expectations and experiences (ACHCEW contri bution). In: Privacy in the Electronic NHS. (Debate organised by the British Medical Informatics Society, London, 30 November 2000.) (www.bmis.org/privacy 2000/chester.doc). (Accessed 10 April 2003.)

13 Confidentiality and Security Advisory Group for Scotland (2002) Protecting Patient Confidentiality final report. Scottish Executive Health Department. (www.show.scot.nhs.uk/sehd/publications/ppcr/ppcr.pdf). (Accessed 6 August 2003.)

14 Information Commissioner (1998) Data Protection Act 1998: legal guidance. Version 1. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Legal Guid ance'. (Accessed 30 March 2003.)

15 Information Policy Unit (undated) Pseudonymisation of Patient Level Data a toolkit for requestors and providers of data. Department of Health, London.

16 British Medical Association (1999) Confidentiality and Disclosure of Health Infor mation. BMA, London.

17 Starr P (1999) Privacy and access to information: striking the right balance in healthcare. In: Massachusetts Health Data Consortium, 4th Annual Meeting, Boston, MA, 16 April. (www.nchica.org/HIPAAResources/Samples/privacylessons/ P-101%20Massachusetts%20Health%20Data%20Consortium.htm). (Accessed 13 September 2003.)

18 Institute of Medicine (1994) Health Data in the Information Age. National Academy Press, Washington DC.

19 Medical Research Council (2000) Personal Information in Medical Research. (Updated January 2003.) (www.mrc.ac.uk/pdf-pimr.pdf).

20 Department of Health (DoH) (2002) Confidentiality: a code of practice for NHS staff (draft),

11 Freedom of information

1 UK Government White Paper (1997) Your Right to Know: the Government's proposals for a Freedom of Information Act. (www.archive.official-documents. co.uk/document/caboff/foi/foi.htm). (Accessed 11 September 2003.)

2 Department for Constitutional Affairs (1997) Open Government: the code of practice on access to government information, (www.lcd.gov.uk/fo i/ogcode981.htm). (Accessed 11 September 2003.)

3 Abraham J, Sheppard J and Reed T (1999) Rethinking transparency and accountability in medicines regulation in the United Kingdom. British Medical Journal. 318: 46.

4 McKee M (1999) Secret government revisited. British Medical Journal. 318:1712.

5 Lord Chancellor's Department (1997) Your Right to Know: background material. (www.lcd.gov.uk/foi/bg_cont.htm). (Accessed 11 September 2003.)

6 Lord Chancellor's Advisory Group on Implementation of the Freedom of Information Act (2002) Annual Report on Bringing Fully into Force those Provisions of the FOIA 2000 which are Not Yet Fully in Force, (www.lcd.gov.uk/foi/ impgroup/foiag02-17.pdf). (Accessed 9 September 2003.)

7 NHS Executive (1999) Code of Practice on Openness in the NHS. (www.doh.gov.uk/nhsexec/codemain.htm). (Accessed 15 September 2003.)

8 The Caldicott Committee (1997) Report on the Review of Patient-identifiable Information. NHS Executive, (www.doh.gov.uk/confiden/crep.html). (Accessed 5 August 2003.)

9 Lowe M, British Medical Association (1998) Letter to R Cayzer, Freedom of Information Unit, 27 February. On: 'Have Your Say' website: responses to the government's FOI consultation paper, (http://foi.democracy.org.uk/html/ submission303.html). (Accessed 15 September 2003.)

10 Derek D, NHS Confederation (1998) Letter to D Clark, Chancellor of the Duchy of Lancaster, 26 February. On: 'Have Your Say' website: responses to the government's FOI consultation paper, (http://foi.democracy.org.uk/html/ submission342.html). (Accessed 15 September 2003.)

11 Information Commissioner (2003) The Freedom of Information Act 2000: an introduction. Office of the Information Commissioner, Cheshire.

12 Campaign for Freedom of Information (2003) Broken Commitments on Access to Health Records, (www.cfoi.org.uk/dohltrl00103.html). (Accessed 15 September 2003.)

13 Information Commissioner (2001) Freedom of Information Act 2000: media brief. Office of the Information Commissioner, Cheshire.

14 Lord Chancellor's Department (2002) Code of Practice on the Discharge of Public Authorities' Functions under Part 1 of the Freedom of Information Act 2000 dealing with requests for information, (www.lcd.gov.uk/foi/codesprac.htm). (Accessed 16 September 2003.)

12 The best way forward

1 Confidentiality and Security Advisory Group for Scotland (2002) Protecting Patient Confidentiality final report. Scottish Executive Health Department. (www.show.scot.nhs.uk/sehd/publications/ppcr/ppcr.pdf). (Accessed 6 August 2003.)

2 Cambridge Health Informatics Limited (2001) Gaining Patient Consent to Dis closure. (www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf). (Accessed 13 March 2003.)

3 Information Policy Unit (2002) Options for the Pseudonymisation of Patient Iden tifiable Information (Draft) Version 1.1. Department of Health, London.

4 Information Commissioner (1998) Data Protection Act 1998: legal guidance. Version 1. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Legal Guid ance'. (Accessed 30 March 2003.)

5 General Medical Council (2000) Confidentiality: protecting and providing infor mation. GMC, London.

6 Medical Research Council (2000) Personal Information in Medical Research. (Updated January 2003.) (www.mrc.ac.uk/pdf-pimr.pdf).

7 British Medical Association (1999) Confidentiality and Disclosure of Health Infor mation. BMA, London.

8 NHS Information Authority, The Consumers' Association, Health Which? (2002) Share with Care people's views on consent and confidentiality of patient information. (www.nhsia.nhs.uk/confidentiality/pages/docs/swc.pdf). (Accessed 20 August 2003.)

9 Information Commissioner (2002) Use and Disclosure of Health Data. (www.dataprotection.gov.uk/dpr/dpdoc.nsf), under 'Compliance Advice'. (Accessed 10 May 2003.)

10 NHS Information Authority (1998) Information for Health, (www.nhsia.nhs.uk/ def/pages/info4health/contents/asp). (Accessed 10 June 2003.)

11 Department of Health (DoH) (2001) Building the Information Core: protecting and using confidential patient information a strategy for the NHS. (www.doh.gov.uk/ ipu/confiden/strategyv7.pdf). (Accessed

10 June 2003.)

12 Department of Health (DoH) (2002) Confidentiality: a code of practice for NHS staff (draft),

13 NHS Information Authority (2002) Caring for Information model for the future.

14 Department of Health (DoH) (2001) Building the Information Core implementing the NHS plan, (www.nhsia.nhs.uk/pdf/info-core.pdf). (Accessed 10 June 2003.)