Clinicians' knowledge and practice of data protection legislation and information management

F. S. Ryan,[1] M. K. Cedro,[2] S. Pabari,[3] L. Davenport-Jones[4] and J. H. Noar[5]

IN BRIEF

- This paper reviews the current legislation and guidance on patient identifiable information.
- Information governance is an integral part of clinical governance and it is incumbent on all clinicians to be aware of their duties toward their patients.
- Clinicians are encouraged to audit their own knowledge and practice of information management and to set up local guidelines.

RESEARCH

Aims The aim of this study was to review current legislation and guidance on information governance and to audit clinicians' management of confidential patient information and knowledge of published guidelines in a teaching hospital. **Materials and methods** A questionnaire was developed based on published Department of Health, General Dental Council and National Health Service guidance. This was then piloted and distributed to clinicians to complete. **Results** A review of the current guidance revealed many confusing and unclear areas. However, clinicians' knowledge of information governance was generally good, with an overall correct response rate of 73%. **Conclusions** All clinicians have an ethical and legal obligation to protect confidential patient data and to be aware of their responsibilities. Local guidelines need to be clarified to help clinicians to manage patient data effectively.

INTRODUCTION

Patient information can be defined as anything that is used to identify a patient either directly or indirectly and is bound by legal and ethical obligations of confidentiality.[1] Information offered in confidence should not be utilised or disclosed in any way that might identify a patient without his or her explicit consent. Some exceptions to this rule do exist but it applies in most circumstances. A duty of confidence:

a) Is a legal obligation derived from case law
b) Is an ethical requirement established with professional codes of conduct, and
c) Must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.[2]

[1*-3]Specialist Registrars in Orthodontics, [4]FTTA in Orthodontics, [5]Consultant/Honorary Senior Lecturer in Orthodontics, Eastman Dental Hospital, University College Hospitals NHS Foundation Trust, 256 Gray's Inn Road, London, WC1X 8LD
*Correspondence to: Ms Fiona S. Ryan
Email: fionaryan25@hotmail.com

Online article number E4
Refereed Paper – accepted 22 July 2008
DOI: 10.1038/sj.bdj.2009.53
©British Dental Journal 2009; 206: E4

The concept of clinical governance was introduced by the Department of Health in 1998 and is defined as 'a framework through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which excellence in clinical care will flourish'.[3] The management of confidential patient information is central to the principles of clinical governance and its importance is highlighted by the fact that it is outlined twice in the Department of Health's ten point list on the main components of clinical governance.[3]

The Caldicott Committee was set up by the Department of Health as a result of concerns that had arisen about the security of patient-identifiable information. It reviewed all such information that passed between the National Health Service (NHS) and other NHS or non-NHS bodies. The Caldicott Report (1998) highlighted weaknesses in the way confidential patient data was handled in the NHS and suggested six principles to govern the use of patient information (Table 1).[4] The Caldicott Principles incorporate the Data Protection Act (1998), which governs the use of personal information through eight principles (Table 2).[5]

In early 2007, the government announced that prison sentences are to be introduced for the first time for certain offences under the Data Protection Act,[5] and while there would have to be a major breach of the Act to incur such a sentence, it is clear that an increasingly stringent approach is being taken.

MATERIALS, SUBJECTS AND METHODS

Questionnaire development

Following a review of current guidelines regarding information management within the NHS, a questionnaire was developed to audit clinicians' knowledge of these guidelines. Using published guidance as a reference, 19 multiple choice questions and answers were devised (Appendix 1).[1-10] The questionnaire was piloted on five members of staff for readability and ease of administration and minor wording changes were made following this.

The gold standard that we set for this audit was 100% correct response rate and the audit standard we chose, which is a more realistic measure, was 90% correct answers overall.

Participants

The questionnaire was distributed to all NHS clinical members of staff in the Orthodontic Department at Eastman Dental Hospital during a meeting, and participants were given 30 minutes to complete the questionnaire under exam conditions. A mixture of NHS consultants, orthodontic specialist practitioners and specialist registrars in orthodontics participated.

RESULTS

The results of the questionnaires are presented in this section; each question is listed together with the right answer and the percentage of participants who responded correctly. For some questions a definitive answer does not exist and these are considered in more detail.

Figure 1 illustrates the numbers of completed questionnaires by designation. The specialist registrar/orthodontic postgraduate constitutes the largest group in the orthodontic department, hence accounting for the majority of completed questionnaires.

Question 1

How long should patient data be stored on my computer, after it is no longer required?

Correct answer: no longer than is necessary in accordance with the Data Protection Act, 1998.

This question was answered correctly by 45% of respondents (Fig. 2).

Question 2

If you are approached by the police for information regarding one of your patients, can you provide it?

Correct answer: yes, but they must confirm that it is to prevent or detect serious crime, or to apprehend or prosecute offenders. The release of the information is at your discretion except if the police produce a court order.

70% of respondents answered this question correctly (Fig. 3).

The answer to this question is not entirely clear. As stated in *Confidentiality: NHS code of practice* issued by the Department of Health in 2003, 'the definition of a serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.'[1]

The police are not automatically entitled to access to personal patient data unless they produce a court order. When considering such a breach, the clinician must satisfy him or herself that there is a definite public interest justification and document it clearly in the patients' notes. In addition, care must be taken that only the minimum data is revealed. If in doubt, advice from your defence organisation or trust should be sought.

Question 3

The mother of a 17-year-old patient telephones and enquires whether her son has been attending his appointments

Table 1 The Caldicott Principles of personal data use within the NHS

The Caldicott Principles
• Justify the purpose(s)
• Do not use patient-identifiable information unless it is absolutely necessary
• Use the minimum necessary patient-identifiable information
• Access to patient-identifiable information should be on a strict need to know basis
• Everyone should be aware of their responsibilities
• Understand and comply with the law.

Table 2. The Data Protection Principles

All personal information should be:
• Processed fairly and lawfully
• Processed for one or more specified and lawful purposes, be adequate, relevant and not excessive
• Accurate and, where necessary, kept up to date
• Kept for no longer than is necessary for the purpose for which it is being used
• Processed in line with the rights of individuals
• Kept secure with appropriate technical and organisational measures taken to protect the information
• Not transferred outside the European Union unless there is adequate protection for the personal information being transferred.

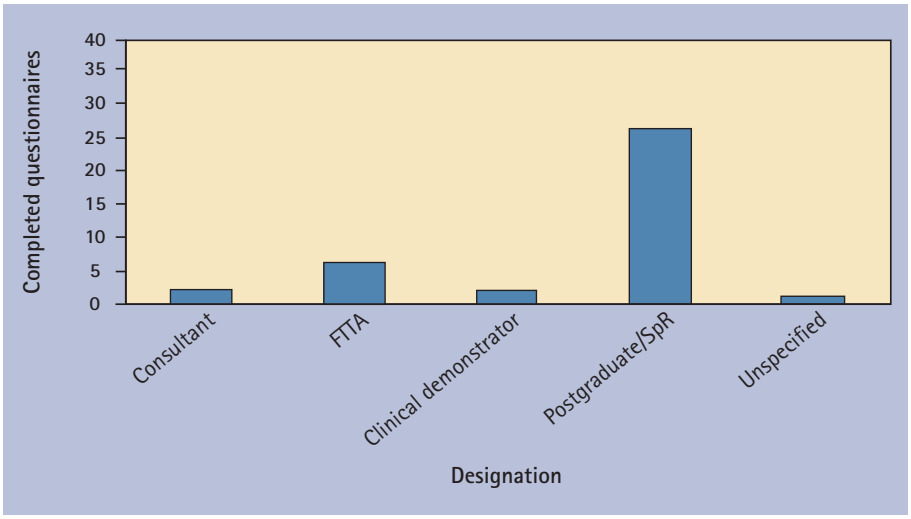

Fig. 1 Number of completed questionnaires by design

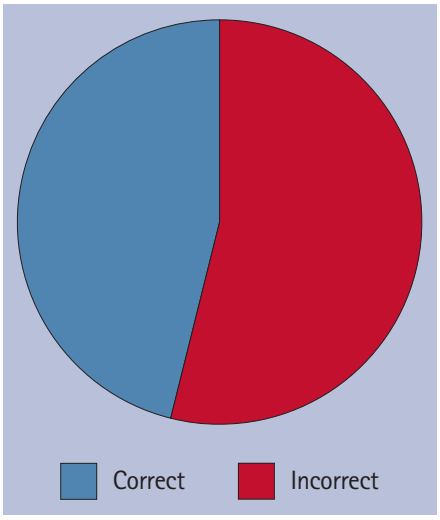

Fig. 2 Proportion of correct responses for Question 1

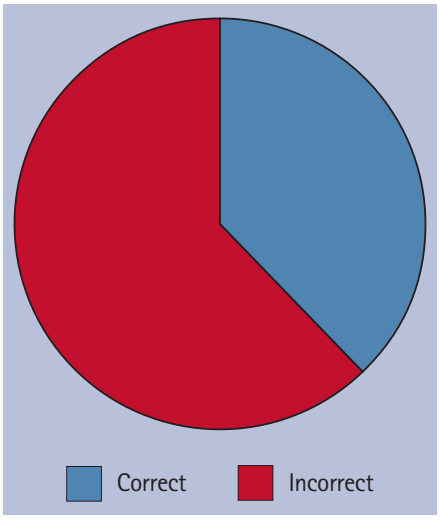

Fig. 4 Proportion of correct answers for Question 4

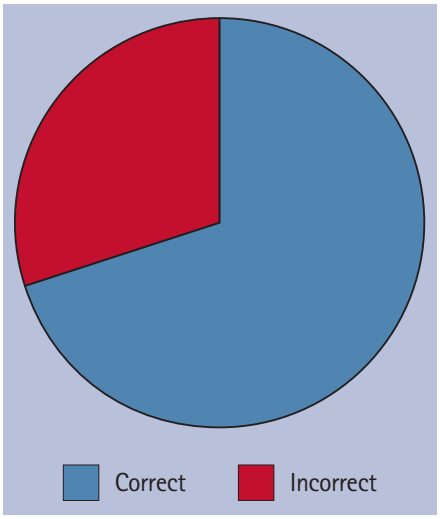

Fig. 3 Proportion of correct responses for Question 2

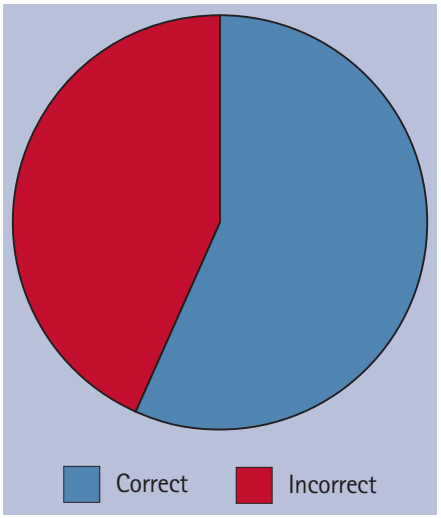

Fig. 5 Proportion of correct responses for Question 9

with you (he always attends alone). What do you do?

Correct answer: decline, explaining that the information is confidential and can only be provided if authorised by her son.

This was a well answered question with 89% of respondents obtaining correct answer.

General Dental Council guidance highlights the importance of protecting the confidentiality of patients' information.[6] In the United Kingdom, 16 is the legal age of consent, and this patient can therefore receive dental or medical care without his parents' knowledge.

In addition, if a patient is under 16 years of age but has demonstrated insight and understanding into their treatment and its' implications (Gillick competent)*, only they can consent to treatment or information about their treatment being disclosed. However, it is advisable to encourage the patient to seek support from their parents where appropriate.

Question 4

If research data is stored on your laptop and all patient data is anonymised, will the Data Protection Act still apply to you?

Correct answer: no.

Thirty-seven percent of respondents answered this question correctly (Fig. 4).

The Data Protection Act does not apply to anonymised data. In addition, *Confidentiality: NHS code of practice* states 'anonymised information is not confidential and may be used with relatively few constraints'.[1]

Question 5

You are going on holiday outside the EU and would like to take your laptop with you (containing patient information) and you are data protected. Are there any restrictions to the transfer of such data outside the EU?

Correct answer: yes, personal data should not be transferred outside the EU without the assurance of adequate data protection, compliance with the act and that the personal data is registered for processing.

This question was answered correctly by 72% of respondents.

Question 6

The envelopes used in postal correspondence with patients should be:

Correct answer: marked strictly private and confidential and any NHS/practice logos and addresses must not be visible.

This question was answered correctly by 37% of respondents.

The General Dental Council specify that confidential information should be protected when 'you receive it, store it, send it or get rid of it.'[6]

Question 7

When calling patients to the surgery, you should ideally:

Correct answer: collect the patient and escort them to the surgery.

This question was answered correctly by 81% of respondents.

Question 8

Which filing system offers the most protection?

Correct answer: a computerised system with access control security and responsible users who apply the Data Protection and Caldicott Principles.[2,4,5]

This was a well answered question with 91% of respondents obtaining a correct answer.

Question 9

Should a wife be informed that her husband is HIV positive, when she does not know and her husband specifically demands she is not told?

*Gillick v West Norfolk and Wisbech Health Authority [1986] AC 112.

Correct answer: yes, in exceptional circumstances, in the interest of public wellbeing.

This question was answered correctly by 56% of respondents (Fig. 5).

According to the *Confidentiality: NHS code of practice* document issued by the Department of Health, 'risk of harm disclosures to prevent serious harm or abuse warrant breach of confidence'.[1] However, this is a contentious issue and anybody in this position should seek advice from their defence organisation.

Question 10

A 12 year-old patient's father calls following an appointment his child had with you that he was not present at. He wants to know what happened at the appointment. What should you do?

Correct answer: tell him you cannot discuss this over the phone, but would be happy to give him details if he comes to the clinic.

Fifty-six percent of respondents answered this question correctly (Fig. 6).

When receiving telephone calls, the health professional should always confirm the identity of the person they are speaking to. Ideally, if someone has called you and you are not sure who they are, it is advisable to ring them back. The other factor that should be taken into consideration is the impact of disclosing this information. Furthermore, it may be that the father does not have parental responsibility. The Children Act (2004) states that parental responsibility is held by the child's parents if they are married to each other or have jointly adopted a child, or the child's mother, but not father, if they are not married. Exceptions to this are if the father has acquired parental responsibility via a court order or the couple subsequently marry. This is not automatically the case for unmarried parents. A father only has this right if he has acquired legal responsibility for his child either by:

- Jointly registering the birth of the child with the mother (after December 1 2003)
- A parental responsibility agreement with the mother
- A parental responsibility order made by a court.

In addition, if the mother dies, parental responsibility does not automatically pass to the father if unmarried.[8]

Question 11

A referring dentist rings you asking for details of a patient's orthodontic treatment plan. What do you do?

Correct answer: write to him with the information.

Eighty-three percent of respondents answered this question correctly.

Confidentiality: NHS code of practice states that 'explicit consent is not usually required for information disclosures needed to provide healthcare. Even so, opportunities to check that patients understand what may happen and are content should be undertaken'.[1]

Question 12

A patient asks to have a copy of their notes. What should you do?

Correct answer: tell them to contact the medical records department.

Eighty-nine percent of respondents answered this question correctly.

Under the Data Protection Act (1998) patients have a right to see and/or have copies of their medical and dental records.[5]

Question 13

Is it permissible for Trust staff to store patient photographs on password protected computers or laptops?

Correct answer: yes it is, but there are specific requirements in the local information governance policy and the Data Protection Act (1998). Ideally the data should be held on CD or memory stick and stored separately from the laptop.

This was answered correctly by 86% of respondents (Fig. 7).

Question 14

Hospital notes must be kept on Trust/practice property.

Correct answer: True, with exceptions.

This was a well answered question with 91% of respondents obtaining the correct answer.

Confidentiality: NHS code of practice supports this answer and states that 'staff should not normally take patient records home'.[1] However, the statement continues to state 'that where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed', demonstrating that the guidelines are not always entirely clear and clinical judgement should be used for each case.

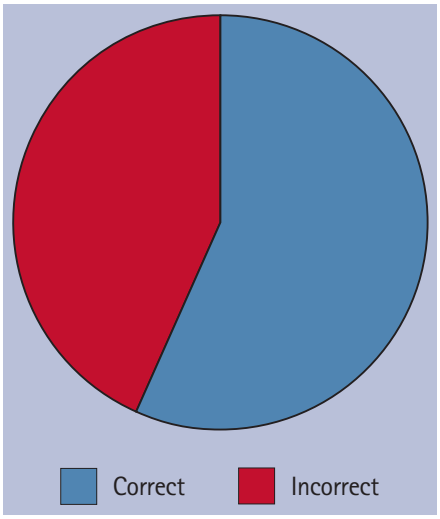

Fig. 6 Proportion of correct answers for Question 10

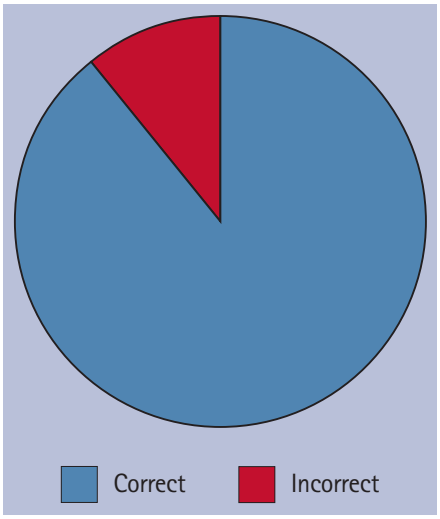

Fig. 7 Proportion of correct responses to Question 13

Question 15

Is it permissible to keep a personal diary of a patient's appointments and contact details?

Correct answer: it is and disposal should be done securely in accordance with the Data Protection Act.

Fifty-nine percent of respondents answered this question correctly.

Question 16

Are you currently personally registered with the Data Protection Register? If so, what is your number?

Twelve respondents (32%) were registered with the Data Protection Register.

Whether or not clinicians need to be individually registered with the Data Commissioner as data controllers is not straightforward and depends for what purposes the information is being or is intended to be used. The definition of a data controller is 'a person who alone, jointly or in common with other persons determines the purposes for which and the manner in which any personal data are processed or are to be processed.' The data controller is required to register with the Information Commissioner. When working in a hospital department, the Trust should be registered and ultimate responsibility lies with the Caldicott Guardian when patient data is used for NHS purposes. However, although such employees will not be classed as data controllers, they will have a contractual obligation to abide by the data protection principles.[10]

Within a practice setting, unless working as an assistant or locum practitioner, all dentists, whether a principal, partner or associate, are advised by the British Dental Association to be individually registered as they are responsible for their patients' clinical records.[10] In addition, every practice must have a data protection policy, a confidentiality policy and an information policy in place.[10]

When using confidential data for any other purposes than the delivery of healthcare, for example teaching/lecturing, examinations or research, explicit written consent should be sought from the patient and the clinician should be registered.

Question 17

This question asked respondents to specify what they considered to be patient identifiable information out of name, address, postcode, photos and NHS number.

All of these were patient identifiable details and most respondents recognised this. However, out of 37 respondents, 10 did not consider a postcode to be patient identifiable information (Fig. 8).

Other patient identifiable markers include videos, audiotapes, rare diseases, drug treatments and even statistical analyses.

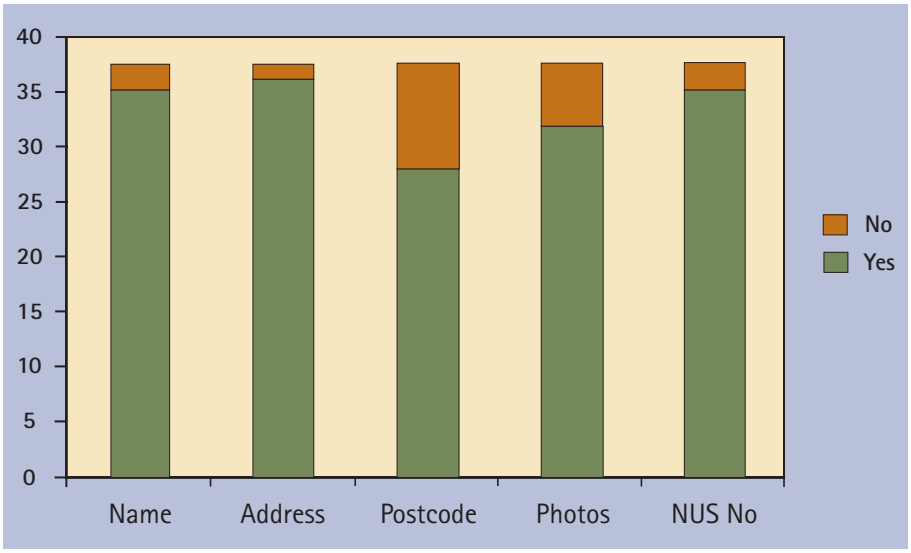

Fig. 8 Correct responses to Question 17 – patient identifiable information

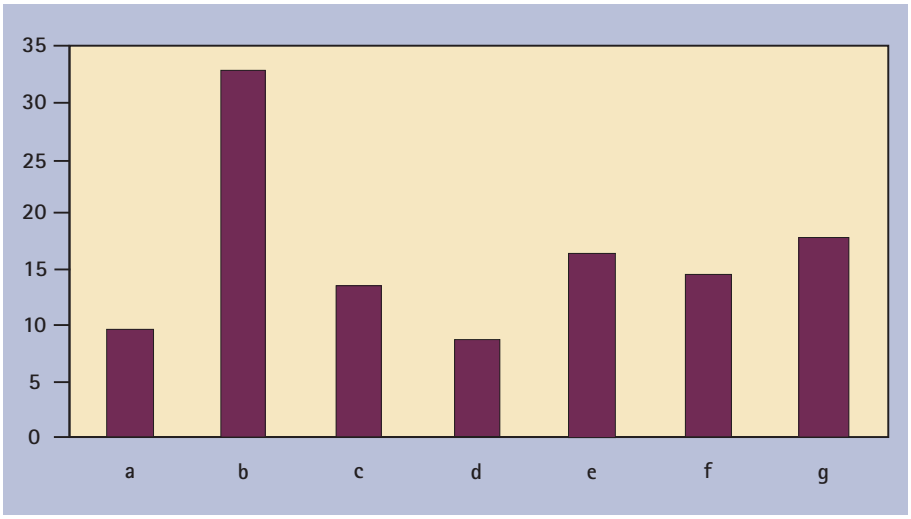

Fig. 9 Responses to Question 19

Question 18

Keeping confidential patient information secure is:

Correct answer: a legal, ethical and NHS contractual obligation.

Eighty-six percent of respondents answered this question correctly.

The General Dental Council's document *Principles of patient confidentiality* in its opening pages states that a dentist has an 'ethical and legal duty to keep patient information confidential'.[6] The Department of Health also states that 'patient information is generally held under legal and ethical obligations of confidentiality'.[1]

Question 19

This question asked respondents to specify which guidelines/regulations they were familiar with concerning information governance.

Most (86%) respondents were aware of the Data Protection Act (1998) and the least (21%) were aware of Trust Law (Fig. 9).

DISCUSSION

This audit was carried out as it was apparent that there was confusion among clinicians regarding the correct protocol with respect to information governance in our department. However, a review of current Department of Health, NHS and General Dental Council guidelines, together with local Trust policy, revealed that there are many areas where absolute guidance cannot be given and a combination of policy and clinical judgment must be exercised. In many of the scenarios listed in the questionnaire, the correct answer may be obvious. However, it is important to understand the guiding principles behind such decision-making.

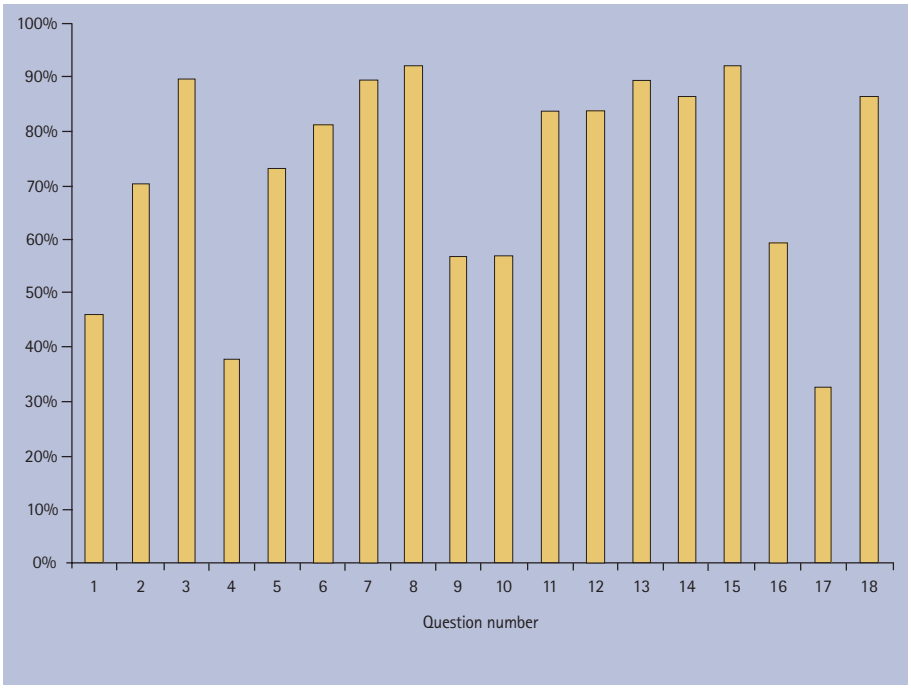

Fig. 10 Percentage of correct answers for each question

The source documents used for the scenarios were lengthy and quite difficult to read and there is often conflicting information in these complex documents. Furthermore, many Department of Health/Trust policies refer to 'locally agreed policy' which does not actually exist or is not published, and exemptions and exceptions apply to many principles but are not, in fact, specified.

Having said that, knowledge of information governance exhibited by the clinicians within this department was quite good. Figure 10 depicts the percentage of correct answers to all questions. Most questions were answered fairly well, with few falling below the 50% mark. This was perhaps more to do with good clinical judgement rather than explicit knowledge or understanding of published guidelines, as the responses to Question 19 reveal. In addition, the overall percentage of correct answers (73%) does fall below the 90% standard for this audit.

Questions 1, 4 and 17 were the worst answered questions. Questions 1 and 4 enquired about electronic data storage. This is a relatively new medium of storage and is increasing rapidly, so it is imperative that clinicians are up to date with the legislation. Question 17 asked if participants were registered with the Office of the Information Commissioner and only 32% were. This perhaps reflects the ambiguous nature of the legislation and guidance surrounding this matter and the differences in whether clinicians work in a hospital or practice setting. However, where in doubt, we would suggest that clinicians contact the Office of the Information Commissioner.

To improve local knowledge and due to the limitations of the published guidance on information governance, locally agreed, concise guidelines are being devised for our department. Once finalised, these will be published and distributed to all clinical staff and this audit will be repeated. Clinicians must also be aware that legislation and policy are subject to change and should endeavour to remain up to date at all times.

CONCLUSIONS

Clinicians' knowledge and practice of information governance principles in our department was good, with an overall correct response rate of 73%. However, there is scope for improvement and as dentists, we are continually being trusted with confidential patient information. Thus it is imperative that all practitioners are aware of their ethical, legal and contractual obligations towards their patients.

We would like to thank Shane Murphy, Information Governance Manager at UCLH, for his help with the development of the questionnaire.

1. Department of Health. *Confidentiality: NHS code of practice.* London: Department of Health, 2003.
2. Department of Health. Patient confidentiality webpage. http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084181 (accessed 30 October 2008).
3. Department of Health. *Clinical governance: in the new NHS.* London: Department of Health, 1999. HSC 1999/065.
4. Department of Health, NHS Executive, Quality and Consumers Branch. *Implementing the Caldicott Report: consultation document.* London: Department of Health, 1998.
5. Office of Public Sector Information. *The Data Protection Act, 1998.* London: The Office of Public Sector Information, 1998.
6. General Dental Council. *Principles of patient confidentiality.* London: General Dental Council, 2005.
7. Office of Public Sector Information. *Health and Social Care Act, 2001.* London: The Office of Public Sector Information, 2001.
8. Office of Public Sector Information. *Children Act, 2004.* London: The Office of Public Sector Information, 2004.
9. Office of Public Sector Information. *Computer Misuse Act, 1990.* London: The Office of Public Sector Information, 1990.
10. British Dental Association. *Data protection.* London: British Dental Association, 2000. Advice Sheet B2.

Appendix 1 Data protection questionnaire

Year/Grade

Please read the following questions and **circle** or **tick** the **single correct answer** unless otherwise specified answers as appropriate.

1) How long should patient data be stored on my computer, after it is no longer required?
a) 10 years because there is no specific guidance and this is best practice operationally
b) 5 years at least because its mandatory to save patient data this long in accordance with the Data Protection Act, 1998
c) No longer than is necessary in accordance with the Data Protection Act, 1998

2) If you are approached by the Police, for information regarding one of your patients, can you provide it?
a) No, never
b) Yes, any information required in a criminal investigation must be provided
c) Yes, but they must confirm that it is to prevent or detect crime, or to apprehend or prosecute offenders. The release of the information is at your discretion except if the Police produce a court order.
d) Only with the patients permission

3) The mother of a 17-year old patient telephones and enquires whether her son has been attending his appointments with you (he always attends alone). What do you do?
a) Give her full information regarding his attendance
b) Decline, explaining that the information is confidential and can only be provided if authorised by her son
c) Send her the details of his attendance in writing

4) If research data is stored on your laptop and all patient data is anonymised, will the Data Protection Act still apply to you?
a) Yes, without any exemptions
b) Yes, but with certain exemptions
c) No

5) You are going on holiday outside the EU and would like to take your laptop (containing patient information) with you and you are registered under the Data Protection Act. Are there any restrictions on the transfer of such data outside the EU?
a) Yes, patient data should never transferred outside the UK
b) Yes, personal data should not be transferred outside the EU without the assurance of adequate data protection compliance with the Act and that the personal data is registered for processing
c) No, there are no restrictions to the transfer of personal data outside the UK as long as you are registered under the Data Protection Act and same rules apply for EU and non-EU countries

6) The envelopes used in postal correspondence with patients should be:
a) Marked private and confidential on NHS Trust marked envelopes
b) Marked strictly private and confidential and any NHS/practice logos and addresses must not be visible
c) Unmarked
d) Stamped with the department logo

7) When calling patients to the surgery, you should ideally:
a) Call the patient over the loudspeaker using their full name and which room they should come to
b) Collect the patient and escort them to the surgery
c) Ask the receptionist to send the patient to the correct room
d) Ring them on their mobile phone and tell them to come to the surgery

8) Which filing system offers the most protection?
a) Locked drawer storage with hand written records
b) Computerised system with access control security and responsible users who apply the Data Protection and Caldicott Principles
c) One dedicated storage office holding all patient records
d) On a Carousel in the department reception

9) Should a wife be informed that her husband is HIV positive when she does not know and the husband specifically demands she is not told?
a) Yes, she should be told
b) No, she should not be told
c) Yes, in exceptional circumstances in the interest of public wellbeing

10) A 12 year-old patient's father calls following an appointment his child had with you that he was not present at. He wants to know what happened at the appointment. Do you:
a) Explain the details of the appointment to him
b) Write to him with the information
c) E-mail him with the information
d) Tell him you cannot discuss this over the phone, but would be happy to give him details if he comes to the clinic
e) Explain that you cannot tell him anything without the patient's permission

11) A referring dentist rings you asking for details of a patient's orthodontic treatment plan. Do you:
a) Tell him the information over the phone
b) Write to him with the information
c) Tell him you need to obtain consent from the patient before you can tell him

12) A patient asks to have a copy of their notes. Do you:

a) Photocopy the notes and post them to them

b) Give them the original notes

c) Tell them they can view the notes but not have a copy as they are Trust Property

d) Tell them to contact medical records department

13) It is permissible for Trust staff to store patient photographs on password protected home computers or laptops

a) True, but there are specific requirements in the Information Governance Policy. Ideally the data is to be held on CD or memory stick and stored separately from the laptop.

b) False there are no situations allowed that permit patient data to be held on a laptop

14) Hospital notes must be kept on Trust property

a) True, with exceptions

b) False

15) It is permissible to keep a personal diary of patient appointments and contact details

a) True and disposal should be done securely in accordance with the Data Protection Act

b) False manual records are not covered by the Data Protection Act

16) Are you currently personally registered with the data protection register? If so, what is your number?

a) Yes Number _____

b) No

17) Patient identifiable information is a patient's: (Please tick either Yes or No for **each** option)

	Yes	No
Name	☐	☐
Address	☐	☐
Post Code	☐	☐
Photos	☐	☐
NHS number	☐	☐

18) Keeping confidential patient information secure is: (Please circle/tick the **incorrect** option)

a) A legal obligation

b) An ethical professional obligation

c) An NHS contractual obligation

d) Optional

19) What guidelines/regulations are you aware of or follow concerning data protection/information governance? (Please tick/circle as many options as apply to you)

a) Computer Misuse Act (1990)

b) Data Protection Act (1998)

c) Human Rights Act (1998)

d) Health and Social Care Act (2001)

e) Trust Law (administrative)

f) NHS Code of Confidentiality

g) Records Management NHS Code of Practice

h) Caldicott Principles

i) Other (please specify)

Thank you for taking time to complete this anonymous questionnaire. If you have any comments/suggestions we would be very grateful if you could write them in the space below.