Medical audit

The Data Protection Act 1998: an audit of its effect on surgical trainees' practice

Jill B Webb

Department of Plastic Surgery, City General Hospital, Stoke-on-Trent, UK

The Data Protection Act 1998 came into force in March 2000 and has significant implications on our normal practice. A survey of surgical specialist registrars was made to establish knowledge of the Act and adherence to its eight principles. Knowledge was patchy and adherence minimal. Simple guidelines are suggested to help juniors keep within the principles of the Act.

Key words: Data Protection Act 1998 – Adherence – Survey – Surgical specialist registrars

The Data Protection Act 1998 (DPA) brings UK legislation into line with the European Union (EC Directive 95/46/EC). It concerns written records (*e.g.* medical notes) as well as data held on computer, and has implications on the way we should work. Concern has been raised regarding its impact on research and audit.^{1,2} To comply, we must change the way we handle personal information, *e.g.* surgical logbooks, research or audit data. Surgical specialist registrars working at a general hospital were surveyed to investigate their knowledge and understanding of the implications of the DPA.

Materials and Methods

Surgical specialist registrars employed at North Staffordshire Hospital – NHS Trust were met or telephoned. Questions were asked on the data included in their logbook: where it was kept and whether the information was on computer or paper. Methods of security against theft and accidental disclosure were investigated. A similar set of information was requested about any data that the trainee kept for audit or research.

Enquiries were made of their knowledge of the DPA and their awareness of implications to their daily work. Conversation that followed often gleaned interesting comments, which were also recorded.

Results

Of the 32 specialist registrars, 31 took part in the study (Table 1). All kept a logbook: on paper (8), on computer (17), or both (6). The patient was identified by name (15) or initials (8). The hospital number was included by 24 (75%) trainees. The age was collected by 19 and the date of birth by 7. Seven trainees did not record specific age-related data, but some held imprecise age data, such as adult/child or their decade. Three trainees recorded neither name nor hospital number, which would be difficult to verify should the need arise.

Only one trainee always kept his logbook at work, on a stand-alone personal computer (PC) in theatre. Many members of staff had access to this computer via a screen-saver password. All other trainees kept their log at home (17), on a portable computer (10) or stated that they kept their paper record on them at all times (3).

Correspondence to: Jill B Webb, Department of Plastic Surgery, Shandwell Healthcare NHS Trust, Lyndon, West Bromwich, West Midlands B71 4HJ, UK. Tel: +44 121 553 1831; Fax: +44 121 607 3355; E-mail: jillwebb@doctors.org.uk

Table 1 Distribution of trainees by speciality

Speciality	Number
Surgery	10
General surgery	6
Cardiothoracic surgery	3
ENT	3
Maxillofacial surgery	2
Neurosurgery	2
Plastic surgery	2
Urology	2
Ophthalmology	1

Of the 23 trainees who had their logbook stored electronically, 11 had a 'computer' password (boot-up or Windows) and 6 had the database password protected (5 of whom also had a computer password). Only the theatre computer had a screen-saver password. None used encryption or a firewall. One trainee believed that keeping his laptop in a locked briefcase secured his data. The trainees who kept paper logbooks did not store the information anywhere secure. However, one shredded the daily detailed log every 6 months after creating summary sheets.

Eight trainees had no research or audit projects, or their projects held no patient identifiable information. Of the remaining 23 trainees, 20 (87%) held their data electronically: 3 used a PC at work, 7 mobile computers, and 16 their home computers (some used more than one). Three had passwords on each of the files, two used a screen-saver password, two had a boot-up password, and one a Windows password (some used multiple systems). The remaining 15 (75%) trainees had no security on their data. The 3 trainees who used paper did not use any security measures.

Eight (26%) trainees were aware that the DPA had changed recently and covered paper as well as computer data. One had notified the Data Protection Commissioner.

Two 'knew' that they probably should be registered. Another 'knew' that the information 'wouldn't pass the data protection officer'.

Thirteen (42%) trainees considered data protection when making personal records, but 3 of these admitted they ignore their conclusions. Another was 'paranoid' about data protection; he will not keep his personal details on computer in case of unauthorised access (his log, research and audit information was paper-based, but not kept securely).

For comments made and attitudes to data protection see Table 2.

Discussion

As clinicians, we are dealing with sensitive data. Patient confidentiality is stressed from medical school. However, with printed information or data on computers, that training seems to be ignored. The principles of the Act must be adhered to, and it is our responsibility to understand them (see Table 3). The Data Protection Commissioner investigates complaints, which can lead to unlimited fines or even criminal prosecution. Many guidelines have been provided (*e.g.* by the General Medical Council (GMC)³, British Medical Association⁴, and NHS Executive^{5,6}), but they were not well disseminated. No individual doctor has been prosecuted to date. Hospital trusts have been involved in breaches of the Act, but not charged (*e.g.* inappropriate disposal of information and irrelevant information collected by questionnaires) and procedures were changed.

Patient information obtained through our normal duties belongs to our employing authority. As we are employees, it is not necessary to notify the Commissioner. However, we must comply with the provisions of the Act individually and inform our local hospital data controller of any information we hold. Data obtained while working for a previous employer is covered by their registration, but one has to consider whether the data are still required for its original purpose. Disclosure of sensitive information (*e.g.* medical

Table 2 Comments and attitudes to data protection.

I know I'm breaking the law, but I will continue
The college force us to break the law in order to have verifiable data
I've recently found that we're not covered when we take the data out of the hospital so I ought to be registered
My PC was recently stolen, it made me think about these issues
Anyone could access data at the hospital, so I now keep it at home where it is more secure
My consultant knows what I keep on my log or for research. He takes the responsibility
I use a Windows password to prevent my family from erasing my data rather than data security
I use the surgical logbook, provided by Region, on my PC. There are no passwords and it requires excessive information
I use a commercially available Psion-based programme. It is available through links from my surgical association Web site, but there's no password

Table 3 *The Data Protection Act 1998 principles^a*

1.	Personal data shall be processed fairly and lawfully
2.	Personal data shall be obtained only for limited purposes
3.	Personal data shall be adequate, relevant and not excessive
4.	Personal data shall be accurate
5.	Personal data shall not be kept for longer than is necessary
6.	Personal data shall be processed in accordance with the rights of data subjects
7.	Appropriate security measures shall be taken against unauthorised or unlawful processing and against accidental loss
8.	Personal data shall not be transferred outside the European Economic Area

data) is strictly controlled by the Act and clear guidelines are available from the GMC.

Paper-based data

Most doctors take paperwork home, often allowing relatives free access to sensitive information. This is a breach of the seventh principle (and breaking patient confidentiality). Furthermore, personal data are simply thrown away. Such printed information should be shredded. Facilities for this ought to be readily available within hospitals, and clinicians informed of their existence. Paper-based information should be kept in a locked filing cabinet, not left so that anyone can read it. It should be filed away or shredded.

Electronically recorded data

It is easy to store excessive information on computers. The third principle prevents the collection of data 'just in case it is useful'. The patient name is not relevant for most specialist registrar projects and, therefore, should not be included. Our memories identify patients by name, not by hospital number (which is still personal data), but legally this is probably excessive.

Data should be held no longer than it is required (fifth principle). Once an audit project is completed, the results should be written up and added to the department's audit file. The raw data should be deleted from a home-based computer, but could be retained at work with suitable security.

Research data are exempt from parts of the Act and may be kept indefinitely, though it is still subject to the first principle.⁶ The Medical Research Council has clear guidelines on its Web site (<http://www.mrc.ac.uk>).⁷

The information in our operative logbooks should also be kept to the minimum. As each attachment or job is completed, a suggested procedure is shown in Table 4, but then details would be difficult to verify.

A determined individual will be able to access your data, but 'reasonable' measures should be taken (seventh principle). Particular care must be taken regarding laptop computers and personal digital assistants due to the ease of accidental loss. The Office of the Data Protection Commission help-line was vague as to what 'reasonable' was. It depended on the organisation's budget, the likelihood of 'attack', and the nature of the data being kept. They said that firewall or encryption software was unnecessary for home computers processing data obtained at work. Table 5 shows a suggested security for PCs.

Table 4 *Suggested method of removing excess data at the end of an attachment*

1.	Print a list of procedures (without patient names), together with coding and supervision code for the period at that attachment
2.	Get it signed
3.	Store this list in a secure place
4.	Delete all names and hospital numbers from these records, leaving the procedures and coding available for summaries in the future

Table 5 *Security measures for PCs using Windows*

Include a boot-up password for your computer
Include a read-protect password on all files that have patient information in them ('options' in the 'save as' dialogue box in MS Word and Excel)
Have a Windows password with the user profile option of users being able to customise their preferences, so that other members of the family do not have access to sensitive information
Have a screen-saver password in case you leave sensitive information on the screen when you get called away
Be aware of who is behind you and potentially reading the screen

Conclusions

In general, higher surgical trainees do not consider data protection, despite their frequent audit and research activities. Guidance which is plentiful, complex and often seemingly contradictory,⁹ is not reaching trainees and their practice is not changing. Simple guidelines are needed for the principal data gathering activities that we perform. Then confidence in our procedures rather than defensive or blasé attitudes, can prevail.

References

1. Al-Shahi R, Warlow C. Using patient-identifiable data for observational research and audit. *BMJ* 2000; **321**: 1031–2.
2. Strobl J, Cave E, Walley T. Data protection legislation: interpretation and barriers to research. *BMJ* 2000; **321**: 890–2.
3. General Medical Council. *Confidentiality: Protecting and Providing Information*. London: GMC Publications, 2000.
4. British Medical Association. *Confidentiality and Disclosure of Health Information*. London: BMA, 1999.
5. Lidell A. *Data Protection Act 1998: Protection and Use of Patient Information* (HSC 2000/009). Leeds: NHS Executive, 2000.
6. NHS Executive. *Data Protection Act 1998: Protection and Use of Patient Information*. London: Department of Health, only version at <<http://www.doh.gov.uk/dpa98/>>.
7. MRC Working Group. *Personal Information in Medical Research*. MRC Ethics series, October 2000.
8. Data Protection Registrar. *The Data Protection Act 1998: An Introduction*. London: HMSO, 1998.
9. Dyer C. BMA's patient confidentiality rules are deemed unlawful. *BMJ* 1999; **319**: 1221.