The requirements of the Data Protection Act 1998 for the processing of medical data

P Boyd

Correspondence to: My P Boyd, Assistant Information Commissioner, Information Commissioner’s Office, Wycliffe House, Water Lone, Wilmslow, Cheshire SK9 5AF, UK; mail@dataprotection.gov.uk

Accepted for publication 23 September 2002

The Data Protection Act 1998 presents a number of significant challenges to data controllers in the health sector. To assist data controllers in understanding their obligations under the act, the Information Commissioner has published guidance, The Use and Disclosure of Health Data, which is reproduced here. The guidance deals, among other things, with the steps that must be taken to obtain patient data fairly, the implied requirements of the act to use anonymised or pseudonymised data where possible, an exemption applicable principally to records based research, the right of patients to object to the processing of their data, and the interface of the act and the common law duty of confidence.

In order to clarify the misconceptions that have arisen since the 1998 act was passed the Information Commissioner has now issued some general guidance. This can be found at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf. The guidance is an attempt to clarify the precise requirements of the Data Protection Act. As such its intended readership includes data protection and legal officers, Caldicott Guardians, and those involved in the implementation of information strategies within the NHS. It is not aimed at a general readership. The NHS executive, however, leading work on the development of an NHS wide code of practice which should incorporate not only the standard required by the act but also those of the GMC, BMA, and so on.

In summary, the guidance attempts to describe the conditions that must be satisfied in order to process medical data. Chapter one describes the scope of the guidance. It does not address questions of data quality, rights of access, or security which are also covered by the act.

Chapter two discusses the implications of the first data protection principle, which requires that personal data are processed fairly and lawfully. In particular it explains that the act requires that personal data are processed lawfully. In particular it explains that the act does not make the obtaining of patient consent for the processing of their data a requirement of the act (providing that the data are only processed for medical purposes and that it is necessary to process the data for those purposes). It does, however, require that personal data are fairly collected, which in turn requires that patients must be provided with information as to the purposes for which their data are processed and the identity of those who may have access to those data.

Although consent is not an explicit requirement of the act, it may be an implied requirement in that the act has a general requirement that personal data are processed lawfully. Processing of personal data in breach of a duty of confidence, for instance, would be actionable through the courts and since breaches of confidentiality are unlawful would also be a contravention of the first data protection principle. The guidance does not attempt to describe the case law in any detail. Chapter four, however, discusses the Information Commissioner’s approach to determining whether data may have been processed in breach of a duty of confidence.

Medical research is one of the areas upon which the 1998 act is believed to impact particularly strongly. Chapter three of the guidance examines the implications of the second data protection principle, which requires that personal data are only processed for purposes compatible with those for which they were originally obtained. The chapter then explains how an exemption relating to the processing of data for research...
purposes, together with the first principle rules to be applied when obtaining data from a person other than the data subject, are likely to permit some records based research even though the patient in question may not have been informed of this use of their data.

Although consent is not an explicit requirement of the act, individuals do have a number of grounds upon which they may object to the processing of their personal data. This issue and the use of optouts as means of obtaining consent for secondary uses of data are discussed in chapter five. Finally, appendix one consists of tables of the typical uses of medical data, whether for care and treatment, administrative purposes, research and teaching, or non-medical purposes, together with the particular data protection considerations that must be taken in respect of the different uses.

**DISCUSSION**

Cyril Chantler asked Phil Boyd if patients whose data is in the Public Health Laboratory Service (PHLS) and cancer registries have to give consent for their data to be processed? Is consent implied or is explicit consent necessary? Are there exceptions to the law?

Phil Boyd replied that the only exception to the data protection legislation is in cases that require a statutory declaration.

In other cases, where there will be no prejudice as a result of sharing information, researchers should do so. In most cases implied consent has been given.

Professor Julian Peto expressed deep frustration with the way in which the Data Protection Act is hindering epidemiological research. He said there seems to be a problem in the interpretation of common law, which defies common sense. Whilst he can see that it is possible to obtain consent for data to be entered into a registry for future use from current patients, many of the records used are old. It is just not possible to gain retrospective consent.

Further questions were raised about how you decide on the level of information required before patients can give their consent and it was asked whether all medical data could be classed as sensitive. Phil Boyd pointed out that according to an EU directive, all medical data are sensitive. As for how much information to give patients, he suggested that as long as you have procedures in place to ensure that patients are given information before they give their consent, then if you follow those procedures, you couldn’t be found negligent in the eyes of the law.

The pdf of *The Use and Disclosure of Health Data* can be found as a data supplement at our website [www.dataprotection.gov.uk/dpr/dpdoc.nsf](http://www.dataprotection.gov.uk/dpr/dpdoc.nsf).