

DATA PROTECTION

PART 1: AN OVERVIEW

Jacqueline Gazey is an experienced and ISEB accredited data protection practitioner who has over six years experience in the practical application of privacy law. She has developed procedures, policy and tools to meet the requirements of both the 1984 and 1998 Data Protection Acts.

Jacqueline is the co-author of the BSI guide to Subject Access and has been involved in the regularly held ISEB accreditation training courses, run by the BSI. She frequently writes about the practical application of data protection law for trade publications and specialist periodicals and, as a data protection consultant, has a wide range of experience in delivering practical training, guidance material and compliant working procedures.

This article gives a high level insight to the requirements of the 1998 Data Protection Act and gives some practical advice and examples on how a minimal level of compliance can be achieved simply.

Key words: data protection, eight principles, patient records, privacy, individual's rights

The UK has had legislation to protect personal information since the mid-1980's. However, up until a couple of years ago, the legal requirements placed on business by this legislation were largely ignored by all but the very few. In 1998 new legislation came into force and with it came increased powers of prosecution by the Regulator and greater awareness by the general public as to their rights.

As with the previous legislation¹, the 1998 Act revolves around eight basic principles. However, where the previous act related solely to automated data, the new legislation now covers manually held data if it is kept in a *relevant filing system** - so items such as manual record cards are now captured by the law.

The aim of this article is to highlight the key requirements of the Act and, focusing mainly on the most important

principle, give advice on some simple actions, which will assist optical practitioners to operate within the requirements of the law. For those organisations that wish to take the risk-free approach, however, there is a formal audit process available via the Acts Regulator – The Information Commissioner².

The eight Data Protection principles state that personal information (or personal data) must be:

1. Processed fairly and lawfully.
2. Obtained only for the reasons specified, and not used for any other purposes incompatible with these reasons.
3. Adequate, relevant and not excessive.
4. Accurate and kept up-to-date where necessary.
5. Retained only as long as necessary.
6. Processed in accordance with the rights of the individual (or data subject).
7. Kept secure against unlawful processing, accidental loss, destruction or damage.
8. Retained within the EEA - unless the transfer is to a country that ensures an adequate level of protection.

Principle 1 is probably the most important element of this law. Under this principle a *Data Controller* is not only required to ensure that what he is doing with personal information is lawful but it must also be fair. Fairness is something of an

emotive requirement as it is very difficult to define. However, the Information Commissioner states that to ensure fairness the minimum requirements are that a *Data Controller*:

- Tells an individual who they are
- Advises the individual what they intend to do with the personal information they have collected
- Gives information on any other aspect, which may be required to make the processing fair. In practice, most importantly, this means giving details on who information may be disclosed to and where requests for access to personal information should be made

For most organisations this has translated itself into a 'Fair Collection Notice' which can be found on application forms, contracts or in telephone scripts. In the optical trade – for patient information - it could be as simple as a notice placed strategically over the reception desk for people to see as they enter the practice. Notices for new members of staff may be placed in the confirmation letter or employment contract.

A Fair Collection Notice directed towards optical patients may typically look like the following:

- **Such and Such Opticians is the trading name for ABC Company Limited. ABC will use personal information given by you and received from other sources for the purposes of eye care, medical advice and**

treatment [insert all other uses of data here as well]. The information we hold may be disclosed to the NHS, other optical professionals or medical advisors [add any other key recipients of information]. You are entitled to ask for a copy of the information we hold on you [add details of the fee to be charged, if applicable] and have any inaccuracies corrected. Please contact us at 12 The Street, etc.

If the organisation conducts marketing, you will see something like:

- **ABC may, from time to time wish to contact you about other services or products, which may be of interest to you. If you would prefer not to receive this information, please [let us know]/[tick the box] etc.**

On top of the obligations to ensure fairness, principle 1 also requires that a *data controller* justify the reason for *processing* information and *sensitive* information. The Act gives a list of justifications that could be called upon as the reason for processing. For an optical practice, either the individual's consent would need to be obtained or reliance placed in the justification which basically states that the *processing* is necessary to allow the organisation to pursue its legitimate business interests.

Unfortunately the solution is not so simple when it comes to *processing* 'sensitive' data such as medical information. Again there are a list of justifications given in the Act. For opticians, there are two possibilities. Either, the processing is necessary for medical purposes and is undertaken by a health professional or the optician has obtained the 'Explicit Consent' of the individual. 'Explicit' means that the individual has to be fully informed as to the reason information is processed and then their direct consent is freely given. Whilst the law doesn't say the consent has to be obtained in writing, the Information Commissioner's verbal guidance on this has been that written proof is the best way to protect the organisation. Practically, for opticians who chose to apply the consent approach, written consent may not be the solution. The process for gaining consent may be for the person collecting the information to say why it is required and to simply ask the patient if it is okay. The record card or place where the information is being recorded could then be noted accordingly.

To sum up the requirements of the First Principle:

- Make sure that you advise both patients and staff exactly who you are and why you are *processing* the information
- Have a point of contact for people who may wish to exercise their right of access to the information held about them
- When collecting 'sensitive' information, advise the individual why its

DEFINITIONS

<i>Data:</i>	Information processed (or is intended to be processed) by electronic equipment or recorded (or is intended to be recorded) in a relevant filing systems
<i>Personal data:</i>	Information, which relates to a living individual who can be identified
<i>Processing:</i>	Obtaining, recording, holding, manipulating or the destruction of personal data
<i>Data controller:</i>	The person/organisation that determines the purpose and manner in which personal data are processed - eg the optical practice
<i>Data subject:</i>	The individual who is the subject of the personal data - eg a patient or member of staff
<i>Data processor:</i>	A person or organisation who processes data on behalf of the data controller, under contract to carry out their instructions - eg an external glazing business who may briefly hold patient information.
<i>Sensitive data:</i>	Information relating to physical or mental health, racial or ethnic origin, political or religious opinions, commission (or alleged commission) of any offence, trade union membership.
<i>Relevant filing system:</i>	Non-automated systems for storing personal information in a format which is referenced by individual - eg alphabetical filing of record cards.

needed and ask if it is okay for this information to be *processed*. Record their response with the information.

A less detailed look at the other Data Protection Principles

Principle 2 includes the requirement for every *data controller* to register or notify to the Information Commissioner what personal data they are processing and why. Failure to notify is an offence under the Act, unless an exemption can be applied, and under the old law the majority of prosecutions were for non-registration. Notification can be completed on-line [access through the Information Commissioner's website – www.dataprotection.gov.uk], over the telephone or by post and costs £35 pa per legal entity. The Commissioners office is very helpful in completing notifications and does have a 'template' notification (N815) for opticians. There is, therefore, little need to go via agencies who will charge up to £100+ the £35 notification fee. Notifications are renewable annually and the Information Commission recommends that organisations should take this opportunity to review how they process information to check that their notifications are accurate.

Principles 3, 4 and 5 cover the collection, accuracy storage and retention of data and are called the 'quality principles', as they are not only a requirement of the law, they make good business sense as well. A word of warning, however, about the statement "not excessive" in Principle 3. This means that you cannot collect information just because it may come in useful in the future. Neither does having consent from the individual to hold the excessive information make it OK, it will still be a breach of this principle. Principle 5 is all about having a retention, deletion and disposal policy in place. For optical records, the accepted retention period is 10 years after the last update and organisation should have procedures in place to regularly dispose of information, securely, after this period has expired.

Principle 6 covers the rights of individuals over their personal information. These rights are:

- Right of access to their information
- Right to prevent *processing* which is likely to cause damage or distress
- Right to say no to any form of direct marketing
- Right to be advised where decisions are made solely by automated means – and the right to object
- Right to have inaccurate information blocked, erased or destroyed
- Right to claim compensation for any damage suffered against an organisation that fails to comply with the Act.

Every organisation should have a point of contact who can field requests under these rights and compile information for an individual if they ask for access to the records held on them.

Principle 7 says that a *Data Controller* must provide adequate security around the personal information they hold – giving regard to the harm that may result from loss, destruction or disclosure. For optical practices, this effectively means that members of staff who handle data should be trained in the basic requirements of data protection law. It also means computer records should be covered by password access, which is changed occasionally and regular back-ups should be taken. For manual records, these should be stored in a secure fire-proof environment in an area where they cannot be easily accessed by patients or members of staff who have no need to see them. During use, great care should also be taken to keep the information confidential. For example, do not leave record cards out on the reception desk where they can be overlooked and information disclosed to members of the public.

On the subject of disclosure of information, this Act does not state that you cannot disclose information to other parties, it simply states that you must be sure of the basis on which you carry out this disclosure – for example, do you have the consent of the individual concerned. In the majority of cases, disclosure will be covered by either a requirement under NHS law or the individual's consent. The times where greater care should be taken is where calls are received from other opticians asking for historic information. In these cases, disclosure could take place as it is in the legitimate business interest of the parties concerned. However, ensure you are acting in the individual's best interest and make a note of any disclosure so that you have a record of the transaction should any subsequent query be made.

Principle 8 covers the transfer of information outside the European Economic Area (this being the EEC + Norway, Liechtenstein and Iceland). This is probably a rare occurrence in most practices, however, if a request is made from another country for information on a patient, the most secure way of ensuring compliance with the law is to get the consent of the individual concerned before any information is released.

References

1. The 1984 Data Protection Act.
2. Information Commissioner – Wycliffe House, Water Lane, Wilmslow, SK9 5AF, T 01625 545745
3. * Italic words relate to the 'definitions' outlined in this article. ■