Data Protection Act 1998
Occupational Health Aspects

1 Introduction

The Data Protection Act 1998 (DPA 1998, the Act) repealed the whole of the Data Protection Act 1984. The Act had the effect of extending the definition of data to cover manually recorded information as well as automatically processed data, e.g. computerised records. Because of this the provisions of the Access to Health Records Act 1990, as they apply to data on living individuals, have been repealed and replaced by similar provisions in the DPA 1998. The Access to Health Records Act 1990 still applies in respect of the health records of people who have died so record holders will continue to receive applications under that Act. The entire text of the Act will be found at
http://www.legislation.gov.uk/ukpga/1998/29/contents

The Data Protection (Subject Access Modification) (Health) Order 2000 - (referred to here as SI 2000/413) provides for the partial exemption from the provisions of the Act which confer rights on data subjects to gain access to data held about them relating to their physical or mental health or condition if the data would be likely to cause serious harm to his or any other person's physical or mental health or condition.
http://www.legislation.gov.uk/uksi/2000/413/contents/made

In this article the main text is a commentary on the Act, section by section, with occasional diversions to later sections or schedules if necessary. Comments are made on the wording of the Act as it might relate to a typical occupational health setting, with health professionals making and keeping health records, both on paper and in computerised systems.

The opinions expressed in this document are those of the author, a specialist in occupational medicine. The reader may wish to refer to legal experts for additional information.

2 Definitions

DPA 1998 S1, S68, S69. Other definitions appear in S70 and S71.

Information relating to individuals, which is held in occupational health computer systems *or* paper records, is likely to be classed as **data** either because it can be processed automatically or because it is part of a **relevant filing system** or **accessible record**. Computer systems are the commonest (but not the only) equipment that can process data automatically.

Paper records are likely to form part of a 'relevant filing system' by being in alphabetical order. Even if they are not, they are an 'accessible record' because they are a **health record** as defined in Section 68.

In occupational health the inclusion of information in the definition of 'data' by being a 'health record' (and therefore an 'accessible record') can only apply if the record was made by or for a health professional in connection with the *care* of an individual. The interpretation depends on the occupational health activities (which include preventive medicine, health education and assessment of fitness for work) being classed as *care*. Care is not defined in DPA 1998 but in SI 2000/413 "care includes examination, investigation, diagnosis and treatment".

Section 1(4) and the definition of the term **data processor** suggest that the **data controller** might be the employer, from a legal point of view. In practice the data controller, or their representative, is more likely to

be the manager of the occupational health facility (rather than the administrator) since they *determine* the purpose and manner of processing.

Recommendation 1: *Identify the data controller (or their representative) for the different systems that you have, automated and manual. Ideally this should be a health professional with managerial responsibility.*

A typical example of a 'data processor' might be an external company who handle backups of computerised data or microfiche archived paper occupational health records.

The data are **personal data** because they relate to living individuals *and* contain expressions of opinion or an indication of intentions in respect of the individual. Almost every entry in an occupational health record has some such expression/indication, even if it is just fit/unfit or the next recall date.

If there is no expression of opinion or indication of intention then the data are just data rather than personal data. This is important because the duties placed on the data controller and the rights given to the data subject by the Act are in respect of personal data

The data is counted as being **processed** simply by 'holding' it as well as organising it or consulting it etc. Processing does not depend on automated (e.g. computerised) methods being used.

DPA 1998 S2. In most cases occupational health data are sensitive **personal data** (sensitive personal data are a subset of personal data).

Recommendation 2: *Classify all occupational health records relating to individuals as sensitive personal data.*

3 The Data Protection Principles

DPA 1998 S4, schedules1,2,3.

There are eight data protection principles, which are set out in schedule 1. Schedules 2 and 3 contain special conditions that apply to 'personal data' and 'sensitive personal data' respectively. The data controller has a duty to comply with the data protection principles in relation to all *personal* data.

(Sections 27,28 and 31 contain exemptions to safeguard the public interest e.g. enforcement of law and order, including health and safety law.)

3.1 The Data Protection Principles and Schedules 1-3

The eight principles in the first part of schedule 1 are straightforward and make sense. The second part of schedule 1 goes into much greater detail. It is better to consider schedules 1-3 at this point, in association with section 4, rather than later as they appear in the Act. This makes it easier to understand the exemptions, which are discussed later.

SCHEDULE 1 - THE DATA PROTECTION PRINCIPLES - PART I THE PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.1.1 The first principle - process fairly and lawfully

In order to comply with the first data protection principle (to process data fairly and lawfully) the most stringent conditions apply to the processing of 'sensitive personal data' (information as to his physical or mental condition). In these cases at least one condition from schedule 2 *and* one condition from schedule

3 must be met.

The effect of Schedule 3 is to incorporate the concept of medical confidentiality into the Act. Processing of sensitive personal data must be done with the subjects explicit consent and/or, if necessary for medical purposes, by a health professional or somebody who owes a similar duty of confidentiality. The ethical standards of health professionals are the basis of this condition. It also defines the standard to be required from members of the occupational health team who are not health professionals.

Recommendation 3: *Occupational health data controllers need to consider which condition(s) in schedule 2 and schedule 3 they will meet in order to comply with the first principle.*

To process the data without the subjects consent it could be necessary to show that the processing was *necessary* to comply with 'legal obligation' or protect the 'vital interests' of the subject *and* for 'medical purposes'. 'Medical purposes' includes preventative medicine but would this condition apply to all of the data in the occupational health record? The only certain way to comply with the first data protection principle would be to have the subjects explicit (informed, written) consent. Data controllers might legitimately consider that their processing meets some of the other conditions and that explicit consent is not required - but they might have to justify that decision.

3.1.2 The fifth principle - Keep data no longer than necessary

Occupational health records are often retained for long periods because of:

- Long latency of disease
- Use of information for research (epidemiology)
- Statutory requirement, COSHH, IRR, CLAW, CAW.
- May be required in connection with litigation in the future

Recommendation 4: *Data controllers should consider whether it is necessary to keep occupational health records for as long as they do - and amend their policy if necessary.*

3.1.3 The seventh principle - Technical and organisational measures

Systems will already be in place to ensure that manual health records are kept securely and that access is restricted. Automated data must also be protected. Data controllers have the responsibility to ensure that organisational and technical measures are adequate.

Members of the occupational health team, who are not health professionals and not governed by an ethical code, must be reliable and comply with a confidentiality agreement.

External 'data processors' must be acting on the instructions of the data controller in accordance with a written contract with adequate guarantees. Typical examples would be data back-up, archiving or transportation of data.

Recommendation 5: *Make sure there is a confidentiality policy that covers compliance with professional ethical standards as well as statutory duty under DPA 1998, Access to Medical Reports Act and Access to Health Records Act. Information and training will be required for non-health professionals to ensure that they are reliable.*

Recommendation 6: *Make sure there are adequate organisational and technical measures to ensure the security of data.*

Recommendation 7: *Make sure 'data processors' will comply with the DPA 1998 as you do. They must be acting on the instructions of the data controller and under a written contract.*

3.1.4 The eighth principle - Transfer of information outside the EEA

If employees are transferred overseas their records may go with them. The requirements in schedule 1 for complying with the eighth principle are complex. However the eighth principle does not apply if the data subject gives their consent to the transfer of information (schedule 1 part II para 14 and schedule 4 para 1).

Recommendation 8: : *Obtain consent from the data subject if their occupational health records are to be transferred to another location and then ensure that they are protected to the same standard as in their original location. This will be good practice even if the transfer is within the European Economic Area.*

3.1.5 Comments on Paragraph 2 of Schedule 1, Part II

This is one of the "subject information provisions". The other is Section 7 - The Right of Access to Personal Data.

Personal data cannot be processed fairly unless the subject has, is provided with or has made readily available to him:

- The identity of the data controller or their representative.
- The purposes for which the data are intended to be processed.
- Any other information to ensure the processing is fair.

The paragraph goes beyond the general rights of access in section 7. It implies that data subjects will be proactively given certain information or at least it will be made readily available e.g. publicised, included in a brochure or leaflet, put up on the wall or on a company intranet site etc. Occupational health departments might consider including the information in a confidentiality promise (see below).

Recommendation 9: *Consider what information should be proactively given to or made available to data subjects in order to comply with schedule1,pt II, para2. Consider whether to combine this with obtaining consents if this is a chosen way to comply with schedules 2 and 3. Prepare some information for employees (data subjects) that can be given out at the pre-employment stage and subsequently.*

4 Rights of Data Subjects and Others

DPA 1998 S7

Data subjects can request, in writing, that the data controller provide information about the data that is held, where it came from and what is done with it.

If the data controller has enough information to identify the subject and the information they request, then they must comply with the request within 40 days. The data subject is entitled to receive the information in 'permanent form' and have it explained to them, if necessary.

They do not have to comply with a request to supply information that would identify another individual, unless it is 'reasonable' to do so or the other individual gives their consent (but see below).

Recommendation 10: *Data controllers need to have a procedure for giving data subjects access to personal data if they request it.*

4.1 Data Protection (subject access modification)(health) order 2000

This Order (SI 2000/413) provides for the partial exemption from the provisions of the Act that confer rights on data subjects to gain access to data held about them, if it relates to their physical or mental health. The exemptions have the effect of maintaining legal safeguards that existed under previous legislation.

4.1.1 Disclosure if likely to cause serious harm

Both the Access to Health Records Act 1990 (section 5(1)) and the Access to Medical Reports Act 1988 (section 7(1)) said there was no obligation to disclose information if it was likely to cause serious harm to the physical or mental health of any individual. The Access to Health Records Act 1990 now only applies to the records of people who have died, and the Access to Medical Reports Act 1988 only applies to medical reports, supplied by a medical practitioner for employment or insurance purposes. SI 2000/413 has the effect of retaining the original protection for people's health. An exemption from section 7 of DPA 1998 is conferred by article 5 (1) but only to the extent to which the supply of information to the data subject would be likely to cause serious harm to any person's physical or mental health or condition.

Before deciding whether this exemption applies (and, accordingly, whether to grant or withhold subject access) a data controller who is not a health professional is obliged by articles 5 (2) and 6 (1) to consult the "appropriate health professional" (definition in article 2). This is another reason for the data controller to be a health professional. This obligation to consult does not apply where the data subject has already seen or knows about the information which is the subject of the request (article 6 (1)), nor in certain limited circumstances where consultation (between data controller and health professional) has been carried out prior to the request being made (article 7 (1) and (2)).

4.1.2 Disclosure of information that identifies other individuals

Under the Access to Health Records Act 1990 the requirement was that "access *shall not* be given to any part of a health record" that would identify another individual, unless they had consented or were a health professional involved in the care of the patient.

The Access to Medical Reports Act 1988 uses the less strict "shall not be obliged".

The Data Protection Act 1998 states that the data controller is "not obliged to comply with a request" if it would result in disclosure of information relating to another individual, unless the other individual had consented OR it is reasonable to comply without their consent.

Section 7(4) gives the data controller the option of withholding information, to protect the identity of (or information relating to) another individual, but only in certain circumstances and only to the extent necessary.

If information was withheld the data controller would have to be prepared to show that it was *not* reasonable to release the information without the other individual's consent.

Article 8 of SI 2000/413 modifies section 7 of the Act so that a data controller *cannot* refuse access on the grounds that the identity of a third party would be disclosed in cases where the information is contained in a health record and the third party is a health professional who has compiled or contributed to that health record or has been involved in the care of the data subject in his capacity as a health professional (unless serious harm to that health professional's physical or mental health or condition is likely to be caused, so that the exemption in article 5(1) applies).
It is important to note that there is nothing in the Act to *prohibit* the data controller from disclosing information to the data subject that would identify another individual; it just says that they are not *obliged* to, in certain circumstances.
Recommendation 11: *Procedures for disclosure of information from occupational health records to data subjects should include (a) consideration of whether the disclosure could seriously harm any person's health and (b) what action needs to be taken if the disclosure identifies another individual.*

4.2 Rights of data subjects to influence data processing.

DPA 1998 S10 -15
Subjects can give written notice to the data controller that they do not want their personal data to be processed because it would cause them (or others) unwarranted damage or distress. The subject will not have this entitlement if conditions 1-4 of schedule 2 apply. For example, if the processing is necessary to protect the vital interests of the individual or to comply with a legal obligation. Data controllers might consider that parts of the occupational health records fulfil one or both of these conditions.

(Sections 11 to 13 and 15 deal with rights in respect of direct marketing, automated decision taking, compensation and jurisdiction.)

Data subjects can apply to a court to have inaccurate data, and opinions based on it, rectified.

5 Notification to the Commissioner

DPA 1998 S16,17. Also 18-26
The Data Protection Registrar is now the Information Commissioner

It is an offence for the Data Controller to 'process' data unless the Commissioner has been notified of certain details and an entry has been made in the register. However, if the data are personal data that are not being and are not intended to be processed by equipment operating automatically (e.g. a computer) then there is no requirement to register (S17(2)).

Recommendation 12: *Computerised occupational health records must be registered but manual ones need not be and this will continue to be the case after the end of the transitional periods, (described later).*

6 Exemptions

DPA 1998 S27-39

6.1 Permanent exemptions in the public interest

Part IV of the Act contains a number of exemptions to permit maintenance of law and order and the performance of various statutory functions, including health and safety.

6.1.1 Historical research

Personal data may be further processed for the purposes of historical research. Subject to certain conditions, the data may be kept indefinitely, are not subject to Section 7 of the Act and are exempt from many of the data protection principles (including the need to comply with schedules 2 and 3).

It is unlikely that these exemptions will be relevant to current occupational health records since, although they may be used (processed) for research, that will not be their *only* use. Records of leavers and archived records *might* qualify for the exemptions if there is an intention to use them for research.

If the data are modified so that individuals cannot be identified from them (not even by using other data that is in the data controllers possession) and/or so that they contain no opinions or indications of intentions in respect of the data subjects then they are no longer personal data and the provisions of the Act will not apply.

Recommendation 13: *Identify and segregate occupational health personal data that will be used* only *for research if it is intended to take advantage of the exemptions from parts of the Act for this type of data processing. Alternatively, modify the data so that they are no longer 'personal data'.*

6.1.2 Disclosure required by law

Disclosure may be required by law, by court order or in connection with legal proceedings. S35

7 Unlawful Obtaining or Disclosure of Data

Occupational health departments should already have a confidentiality/disclosure policy. Administrative staff and other members of the occupational health team who are not health professionals, and aren't bound by an ethical code, will have been instructed in the principles of medical confidentiality (see comments on Schedule 3). Section 55 makes it unlawful for a person to obtain or disclose personal data without the *consent* of the data controller. If the data controller is also a health professional then, in giving their consent, they will consider both the law and their professional ethical standards. Of course, no disclosure would be made without the consent of the data subject in any case.

A person cannot be required to supply or provide access to health records in connection with recruitment, employment or contract of services. Any contractual term which purports to impose such a requirement is void. Health professionals will be aware of similar provisions in previous legislation.

8 Summary

In general the provisions with which we are familiar relating to the Data Protection Act 1984, the Access to Health Records Act 1990 and the Access to Medical Reports Act 1988 have continued to apply under the Data Protection Act of 1998. It is important to remember that the Act applies to many types of data, not just health data. Health professionals will comply with additional ethical and professional standards.

The requirement to register and to give data subjects access to computerised databases continues.

The rights of individuals to have access to their paper (manual) occupational health records continues.

There is a requirement for the Data Controller to comply with the new Data Protection Principles.

In certain circumstances the data controller can withhold information that might identify other individuals, but they are not obliged to.

The Act provides some legal underpinning of the concept of medical confidentiality, for example through the conditions in Schedule 3.

The Act seeks to ensure that contractors and other data processors will meet similar data protection standards as the data controller.

Data subjects will have the right to have certain information given to them or made readily available.

9 Recommendations

1: Identify the data controller (or their representative) for the different systems that you have, automated and manual. Ideally this should be a health professional with managerial responsibility.

2: Classify all occupational health records relating to individuals as sensitive personal data.

3: Occupational health data controllers need to consider which condition(s) in schedule 2 and schedule 3 they will meet in order to comply with the first principle.

4: Data controllers should consider whether it is necessary to keep occupational health records for as long as they do - and amend their policy if necessary.

5: Make sure there is a confidentiality policy that covers compliance with professional ethical standards as well as statutory duty under DPA 1998, Access to Medical Reports Act and Access to Health Records Act. Information and training will be required for non-health professionals to ensure that they are reliable.

6: Make sure there are adequate organisational and technical measures to ensure the security of data.

7: Make sure 'data processors' will comply with the DPA 1998 as you do, acting on the instructions of the data controller and under a written contract.

8: Obtain consent from the data subject if their occupational health records are to be transferred to another location and then ensure that they are protected to the same standard as in their original location. This will be good practice even if the transfer is within the European Economic Area.

9: Consider what information should be proactively given to or made available to data subjects in order to comply with schedule1,ptII, para2. Consider whether to combine this with obtaining consents if this is a chosen way to comply with schedules 2 and 3. Prepare some information for employees (data subjects) that can be given out at the pre-employment stage for example:

- The identity of the data controller or their representative, what data is held, why it is held and what is done with it.
- An assurance regarding adherence to professional ethical standards and the data protection principles.
- An assurance that they can have access to their occupational health records and that they will be kept safely.
- A description of the limited extent of information that would normally be given to management or, where the law requires, to Health and Safety Inspectors. Confirm that confidential clinical information will not be disclosed, unless the employee has consented.
- A section for the employee to give their written consent to the keeping of occupational health data. Ideally there should be two copies, one for the employee and one for the data controller.

10: Data controllers need to have a procedure for giving data subjects access to personal data if they request it.

11: Procedures for disclosure of information from occupational health records to data subjects should include (a) consideration of whether the disclosure could seriously harm any person's health and (b) what action needs to be taken if the disclosure identifies another individual.

12: Computerised occupational health records must be registered but manual ones need not be and this will continue to be the case after the end of the transitional periods.

13: Identify and segregate occupational health personal data that will be used only for research if it is intended to take advantage of the exemptions from parts of the Act for this type of data processing. Alternatively, modify the data so that they are no longer 'personal data'.

Occupational Health Confidentiality Promise

Confidentiality is fundamental to the work of all occupational health staff. Occupational health professionals are bound by an ethical code of conduct in the same way that they would be in a hospital or general practice. Other members of the occupational health team understand their responsibility to protect sensitive personal information and have given an undertaking that they will do so.

We keep a record of the work we do so that the Company can comply with health and safety law, protect the health of employees and ensure that people are fit to do their jobs. Sensitive personal information, which relates to your health, is kept in written and computerised records that are confidential. You should be aware that occupational health doctors, nurses and physiotherapists work as a team and may share the information that you give to them, unless you ask them not to.

Your occupational health records will include details of medical examinations and consultations from the time you joined the company onwards. They will also include advice that has been given to management. When we provide any information for managers then this is restricted to an opinion on whether or not a person is medically fit to do a particular task and whether any modifications or restrictions are necessary. Of course, there is some information that is already known outside the occupational health department for example the reasons for absence that appear on a sick note.

If there is ever a need to release any confidential information then we will always obtain your permission first. Normal medical confidentiality will apply.

As well as complying with the ethical codes of health professionals we also comply with the Data Protection Act 1998. This is one of the reasons for giving you the information in this promise. It also gives us the chance to ask you to sign the agreement below to show that you have seen this information and consent to us keeping your occupational health records in the way we have described.

If you want to see your occupational health records or you want more information about our confidentiality policy then you should contact the manager of your occupational health department.

I have read this confidentiality promise and understand the information that it contains. I agree to information about me being kept and used in this way.

Signed

Name

Date