THE EMPLOYMENT PRACTICES DATA PROTECTION CODE:

PART 4: INFORMATION ABOUT WORKERS' HEALTH.

CONTENTS

SECTION 1: ABOUT THE CODE

Our aim:

This Code is intended to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.

Who is the Code for?

The Employment Practices Data Protection Code deals with the impact of data protection laws on the employment relationship. It covers such issues as the obtaining of information about workers, the retention of records, access to records and disclosure of them. Not every aspect of the Code will be relevant to every organisation - this will vary according to size and the nature of its business. Some of the issues addressed may arise only rarely - particularly for small businesses. Here the Code is intended to serve as a reference document to be called on when necessary.

This part of the Code recommends how your organisation can meet the requirements of the Data Protection Act through the adoption of good practice when obtaining and handling information about workers' health.

The Benefits of the Code:

The Data Protection Act 1998 places responsibilities on any organisation to process personal information that it holds in a fair and proper way. Failure to do so can ultimately lead to a criminal offence being committed.

The effect of the Act on how an organisation processes information on its workers is generally straightforward. But in some areas it can be complex and difficult to understand, especially if your organisation has only limited experience of dealing with data protection issues. The Code therefore covers the points you need to check, and what action, if any, you may need to take. Following the Code should produce other benefits in terms of relationships with your workers, compliance with other legislation and efficiencies in storing and managing information.

Following the Code will:

- increase trust in the workplace - there will be transparency about information held on individuals, thus helping to create an open atmosphere where workers have trust and confidence in employment practices.

- encourage good housekeeping - following the Code encourages organisations to dispose of out-of-date information, freeing up both physical and computerised filing systems and making valuable information easier to find.

- protect organisations from legal action – adhering to the Code will help employers to protect themselves from challenges against their data protection practices.

- encourage workers to treat customers' personal data with respect - following the Code will create a general level of awareness of personal data issues, helping to ensure that information about customers is treated properly.

- help organisations to meet other legal requirements - the Code is intended to be consistent with other legislation such as the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA).

- assist global businesses to adopt policies and practices which are consistent with similar legislation in other countries - the Code is produced in the light of EC Directive 95/46/EC and ought to be in line with data protection law in other European Union member states.

- help to prevent the illicit use of information by workers - informing them of the principles of data protection, and the consequences of not complying with the Act, should discourage them from misusing information held by the organisation.

What is the legal status of the Code?

The Code has been issued by the Information Commissioner under section 51 of the Data Protection Act. This requires him to promote the following of good practice, including compliance with the Act's requirements, by data controllers and empowers him, after consultation, to prepare Codes of Practice giving guidance on good practice.

The basic legal requirement on each employer is to comply with the Act itself. The Code is designed to help. It sets out the Information Commissioner's recommendations as to how the legal requirements of the Act can be met. Employers may have alternative ways of meeting these requirements but if they do nothing they risk breaking the law.

Any enforcement action would be based on a failure to meet the requirements of the Act itself. However, relevant parts of the Code are likely to be cited by the Commissioner in connection with any enforcement action that arises in relation to the processing of personal information in the employment context.

Who does data protection cover in the workplace?

The Code is concerned with information that employers might collect and keep on any individual who might wish to work, work, or have worked for them. In the Code the term 'worker' includes:

- applicants (successful and unsuccessful)
- former applicants (successful and unsuccessful)
- employees (current and former)
- agency staff (current and former)
- casual staff (current and former)
- contract staff (current and former)

Some of this Code will also apply to others in the workplace, such as volunteers and those on work experience placements.

What information is covered by the Code?

Information about individuals, that is kept by an organisation on computer in the employment context, will fall within the scope of the Data Protection Act and therefore, within the scope of this Code. However, information that is kept in simple manual files will often fall outside the Act. Where information falls outside the Act, this Code can do no more than offer advice on good information handling practice.

Personal information

The Code is concerned with 'personal information'. That is, information which:

- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and

- identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.

This means that automated and computerised personal information kept about workers by employers is covered by the Act. It also covers personal information put on paper or microfiche and held in any 'relevant filing system'. In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered.

Only a well structured manual system will qualify as a relevant filing system. This means that the system must amount to more than a bundle of documents about each worker filed in date order. There must be some sort of system to guide a searcher to where specific information about a named worker can be found readily. This might take the form of topic dividers within individually named personnel files or name dividers within a file on a particular topic, such as 'Training Applications'.

Processing

The Act applies to personal information that is subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of

activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

Examples of personal information likely to be covered by the Act include:

- details of a worker's salary and bank account held on an organisation's computer system
- an e-mail about an incident involving a named worker
- a supervisor's notebook containing information on a worker where there is an intention to put that information in that worker's computerised personnel file
- an individual worker's personnel file where the documents are filed in date order but there is an index to the documents at the front of the file
- an individual worker's personnel file where at least some of the documents are filed behind sub dividers with headings such as application details, leave record and performance reviews
- a set of leave cards where each worker has an individual card and the cards are kept in alphabetical order
- a set of completed application forms, filed in alphabetical order within a file of application forms for a particular vacancy

Examples of information unlikely to be covered by the Act include:

- information on the entire workforce's salary structure, given by grade, where individuals are not named and are not identifiable
- a report on the comparative success of different recruitment campaigns where no details regarding individuals are held
- a report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals

- a personnel file that contains information about a named worker but where the information is simply filed in date order with nothing to guide a searcher to where specific information, such as the worker's leave entitlement, can be found.

Sensitive Personal Information:

What are sensitive data?

Sensitive data are information concerning an individual's;

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence, or
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive data found in a worker's record might typically be about their;

- physical or mental health - as a part of sickness records
- disabilities - to facilitate adaptations in the workplace
- racial origin - to ensure equality of opportunity
- trade union membership - to enable deduction of subscriptions from payroll

In the context of medical information, cases in which sensitive personal information might be held include;

- information about a worker's medical history obtained in a pre-employment questionnaire or during the course of an interview or examination once employment has commenced
- the results of drug or alcohol tests included in a worker's personnel file

- information about an individual's disabilities held by an employer for equal opportunity purposes
- information about a worker's health revealed through a medical examination carried out as part of an occupational health or private medical insurance scheme

The Act sets out a series of conditions, at least one of which has to apply before an employer can collect, store, use, disclose or otherwise process sensitive data. As medical information is inevitably sensitive data, such data are likely to be held in all the circumstances addressed in this part of the Code.

See Supplementary Guidance, Page 17 which explains more about the conditions for processing sensitive data

What responsibilities do workers have under the Act?

Workers – as well as employers - have responsibilities for data protection under the Act. Line managers have responsibility for the type of personal information they collect and how they use it. No-one at any level should disclose personal information outside the organisation's procedures, or use personal information held on others for their own purposes. Anyone disclosing personal information without the authority of the organisation may commit a criminal offence, unless there is some other legal justification, for example under 'whistle-blowing' legislation.

Of course, applicants for jobs ought to provide accurate information and may breach other laws if they do not. However, the Act does not create any new legal obligation for them to do so.

See Part 2 – Employment Records, Page 15 which explains more about allocating responsibility.

Other Parts of the Code:

The Employment Practices Data Protection Code has three additional parts,

- recruitment and selection – is about job applications and pre-employment vetting.

- employment records – is about collecting, storing, disclosing and deleting records

- monitoring at work – is about monitoring workers' use of telephones, the internet, e-mail systems and vehicles

Each part of the Code has been designed to stand alone. Which parts of the Code you choose to use will depend on the relevance to your organisation of each area covered.

Ask the Information Commissioner for copies of any parts you require or for any further information.

See Supplementary Guidance, Page 25 for contact details or view our website: www.informationcommissioner.gov.uk

Section 2: INFORMATION ABOUT WORKERS' HEALTH

Data protection and information about worker's health.

The Data Protection Act's sensitive data rules come into play whenever an employer wishes to process information about workers' health. These rules do not prevent the processing of such information but limit the circumstances in which it can take place. The processing must also be consistent with the other requirements of the Act. Employers, especially in the public sector, need to bear in mind Article 8 of the European Convention on Human Rights which creates a right to respect for private and family life.

What does this part of the Code cover?

This part of the Code addresses the collection and subsequent use of information about a worker's physical or mental health or condition. Collection will often be done by some form of medical examination or test, but may involve other means such as health questionnaires.

The issues addressed in this part of the Code will arise typically from the carrying out of medical examination and testing or from the operation of an occupational health scheme. This part of the Code is therefore most likely to be of relevance to larger organisations and those with specific health and safety obligations.

Examples of information about workers' health.

This part of the Code applies to information such as:

- a questionnaire completed by workers to detect problems with their health
- information about a worker's disabilities or special needs
- the results of an eye-test taken by a worker using display screens
- records of blood tests carried out to ensure a worker has not been exposed to hazardous substances
- the results of a test carried out to check a worker's exposure to alcohol or drugs
- the results of genetic tests carried out on workers
- an assessment of fitness for work to determine entitlement to benefits or suitability for continued employment
- records of vaccination and immunisation status and history

Outside the Code.

The Data Protection Act only comes into play when personal information is or will be held electronically or recorded in a structured filing system. This will often be the case but sometimes it may not, for example where a line-manager enquires about a worker's health but does not keep, or intend to keep, any record of the conversation, or only keeps a note in a general notebook.

Where samples are taken, as might be the case with drug or alcohol testing, the Code only applies from the point at which samples yield personal information about a worker. This Code does not address consent for any physical intervention involved in taking a sample from a worker in the course of medical testing.

Sensitive Data Rules.

Where information about workers' health is to be processed, one of the Act's sensitive data conditions must be satisfied. There are various conditions. Below we have listed the ones likely to be of most relevance to employers. Employers holding information about workers' health ought to be able to answer 'yes' to one or more of these questions:

- Is the processing necessary to enable the employer to meet its legal obligations, for example to ensure health and safety at work, or to comply with the requirement not to discriminate against workers on the grounds of sex, age, race or disability?

- Is the processing for medical purposes, e.g. the provision of care or treatment, and undertaken by a health professional or someone working under an equivalent duty of confidentiality, e.g. an occupational health doctor?

- Is the processing in connection with actual or prospective legal proceedings?

- Has the worker given consent explicitly to the processing of his or her medical information?

This is not an exhaustive list of all the conditions.

See Supplementary Guidance, Page 17 for more information on these and other sensitive data conditions.

Relying on the worker's consent.

There are limitations as to how far consent can be relied on as a basis for the processing of information about workers' health. To be valid, consent must be:

- Explicit. This means the worker must have been told clearly what personal data are involved and have been properly informed about the use that will be made of them. The worker must have given a positive indication of agreement, e.g. a signature.

- Freely given. This means the worker must have a real choice whether or not to consent and there must be no penalty imposed for refusing to give consent.

See Supplementary Guidance Page 20 for further explanation of what this means in practice.

Impact assessments.

Once a sensitive data condition is satisfied, an employer then needs to be clear that either:

- it is under a legal duty to process information about workers' health, e.g. the duty to monitor workers' possible exposure to hazardous materials under the Control of Substances Hazardous to Health Regulations 2002, or

- the benefits gained from processing information about workers health justify the privacy intrusion or any other adverse impact on them. In other words, the collection and use of information about workers' health must be a proportionate response to a particular problem.

  An 'impact assessment' is a useful tool for employers to use to help them to judge whether the second of the above options applies.

Particularly where medical testing is involved, employers are likely to find it helpful to carry out a formal or informal 'impact assessment' to decide how or whether to collect information about workers' health. This Code does not prejudge the outcome of the impact assessment. Each will necessarily depend on the particular circumstances of the employer. Nor does the Code attempt to set out for employers the benefits they might gain from holding information about workers' health. What it does do is assist employers in identifying and giving appropriate weight to the other factors they should take into account.
An impact assessment involves:

- identifying clearly the **purpose(s)** for which health information is to be collected and held and the benefits this is likely to deliver

- identifying any likely **adverse impact** of collecting and holding the information

- considering **alternatives** to collecting and holding such information

- taking into account the **obligations** that arise from collecting and holding health information

- judging whether collecting and holding health information is **justified**

Purpose(s).

It is important that a realistic assessment is made of the extent to which the collection of health information will actually address the risks it is directed at. Decisions based on, for example, the effect of particular medical conditions on a worker's future employability or the effect of particular drugs on safety should be based on relevant and reputable scientific evidence.

Adverse impact.

Identifying any likely adverse impact means taking into account the consequences of collecting and holding health information, not only for workers, but also for others who might be affected by it, such as a worker's family. Consider:

- how extensive will the intrusion into the private lives of workers and others be as a result of collecting information about their health?

- whether health information will be seen by those who do not have a business need to know, e.g. IT workers involved in maintaining electronic files about workers

- what impact, if any, will the collection of health information have on the relationship of mutual trust and confidence that should exist between workers and their employer?

- whether the collection of health information will be oppressive or demeaning?

Alternatives.

Considering whether it is necessary to collect information about workers' health, and if so how to do this in the least intrusive manner, means asking questions such as:

- can health questionnaires rather than tests be used to obtain the information the employer requires

- can changes in the workplace, for example eliminating exposure to a hazardous substance, remove the need to obtain information through testing

- can medical testing be targeted at individuals who have exhibited behavioural problems that may be drink or drug related, rather than at all workers

- can the collection of health information be confined to areas of highest risk, e.g. can it be directed at a few individuals the nature of whose jobs mean they pose a particular risk rather than at everyone?

- can medical testing be designed to reveal only a narrow range of information that is directly relevant to the purpose for which it is undertaken?

- can access to health information be limited so that it will only be seen by medically qualified staff or those working under specific confidentiality agreements?

Obligations.

Taking into account the obligations that arise from collecting information about workers' health means considering such matters as:

- whether and how workers will be notified about the collection of their health information

- how information about workers' health will be kept securely and handled in accordance with the Act.

See Part 2 – Employment Records, Page 19 for more information on security requirements.

- the implications of the rights that individuals have to obtain a copy of information that has been collected about their health.

See Part 2 – Employment Records, Page 32 which explains more about rights to access.

Justified?

Making a conscious decision as to whether the current or proposed collection and use of health information is justified involves;

- establishing the benefits the collection and use of health information will bring
- considering any alternative method of obtaining these benefits and/or the information needed
- weighing these benefits against the adverse impact
- placing particular emphasis on the need to be fair to individual workers
- ensuring that the intrusion is no more than absolutely necessary
- bearing in mind that health information can be particularly sensitive, that its obtaining can be particularly intrusive and that significant intrusion will not normally be justified unless the employer's business is at real risk of serious damage
- taking into account the results of consultation with trade unions or other representatives, if any, or with workers themselves

Making an impact assessment need not be a complicated or onerous process. Even in the context of health information it may sometimes be enough for an employer to make a simple mental evaluation of the risks faced by his or her business and to assess whether the collection and use of information about workers' health would reduce or eradicate those risks or would bring particular benefits. In other cases the impact assessment will be more complicated, for example where an employer faces a number of different risks of varying degrees of seriousness. In such cases appropriate documentation would be advisable.

Sickness and Injury Records

For the purposes of this Code it is necessary to distinguish between records that include "sensitive data" and those that do not. The term 'sickness record' is therefore used to describe a record which contains details of the illness or condition responsible for a worker's absence. Similarly, an 'injury record' is a record which contains the details of the injury suffered. The term 'absence record' is used to describe a record that may give the reason for absence as 'sickness' or 'accident' but does not include any reference to specific medical conditions. Many employers keep accident records. Such a record will only be an 'injury record' if it includes details of the injury suffered by an identifiable worker.

Sickness and injury records include information about workers' physical or mental health. The holding of sickness or injury records will therefore involve the processing of sensitive personal data. This means one of the conditions for processing sensitive personal data must be satisfied.

Employers are advised as far as practicable to restrict their record keeping to absence records rather than sickness or injury records.

See Supplementary Guidance, Page 17 which explains more about the conditions for processing sensitive data.

SECTION 3: GOOD PRACTICE RECOMMENDATIONS.

There are six sub-sections in this section of the Code:

1. Information about workers' health: general considerations
2. Sickness and injury records
3. Occupational health schemes
4. Information from medical examination and testing
5. Information from drug & alcohol testing
6. Information from genetic testing

The good practice recommendations primarily address activities such as the use of medical examination and testing or the running of occupational health schemes and so are most likely to be relevant to larger organisations and those with specific health and safety obligations. The issues covered, though, could be of relevance to businesses of any size if they keep information about their workers' health.

Detailed notes and examples, aimed mainly at those in larger organisations who are responsible for ensuring that employment policies and practices comply with data protection law, can be found in the Supplementary Guidance. These notes and examples do not form part of this Code.

For Supplementary Guidance go to: www.informationcommissioner.gov.uk

3.1 INFORMATION ABOUT WORKERS' HEALTH: GENERAL CONSIDERATIONS.

Core principles

- It will be intrusive and may be highly intrusive to obtain information about your workers' health.
- Workers have legitimate expectations that they can keep their personal health information private and that employers will respect their privacy.
- If employers wish to collect and hold information on their workers' health, they should be clear about the purpose and satisfied that this is justified by real benefits that will be delivered.
- One of the sensitive data conditions must be satisfied.
- Workers should be aware of the extent to which information about their health is held and the reasons for which it is held.
- Decisions on a worker's suitability for particular work are properly management decisions but the interpretation of medical information should be left to a suitably qualified health professional.

3.1.1 Identify who within the organisation can authorise or carry out the collection of information about workers' health on behalf of the organisation and ensure they are aware of their employer's responsibilities under the Act.

Key points and possible actions

- Those who handle information about workers' health, or who can authorise the collection of such information, should be briefed on the Act and this Code.
- There are non-compliance risks if those lacking proper authority and any necessary training introduce the collection of health information and in particular medical testing.
- Leave the interpretation of medical information to those who are qualified to do this.

3.1.2 If health information is to be collected ensure a sensitive data condition can be satisfied.

Key points and possible actions

- The collection and use of information about workers' health is against the law unless a sensitive data condition is satisfied.
- In general employers should only collect health information where this is necessary for the protection of health and safety, to prevent discrimination on the grounds of disability, to satisfy other legal obligations or if each worker affected has given his or her explicit consent.
- If consent is to be relied on, it must be freely given. That means a worker must be able to say 'no' without penalty and must be able to withdraw consent once given. Blanket consent obtained at the outset of employment cannot always be relied on.
- Consent should not be confined to the testing itself, it should also cover the subsequent recording, use and disclosure of the test results.

See Supplementary Guidance, Page 17 which explains more about the conditions for processing sensitive data.

3.1.3 Identify clearly the purposes behind the collection of information about workers' health and the specific business benefits which it is likely to bring.

Key points and possible actions

- Identify the collection and use of information about workers' health that currently takes place in your organisation.
- Identify any collection or use of information about workers' health that you plan to implement.
- Consider conducting an impact assessment on current or planned collection and use of health information.

See Page 13 for information on how to carry out an impact assessment.

3.1.4 Protect information about workers' health with appropriate security measures. Ensure that wherever practicable only suitably qualified health professionals have access to medical details.

Key points and possible actions

- Managers should not have access to more information about a worker's health than is necessary for them to carry out their management responsibilities. As far as possible the information should be confined to that necessary to establish fitness to work, rather than consist of more general medical details.

- Safety representatives should be provided with anonymised information unless any workers concerned have consented to the provision of information in an identifiable form.

- Unless the general standard of information security in your organisation is sufficiently high, medical information about workers should be separated from other personnel information, for example by keeping it in a sealed envelope, or subject to additional access controls on an electronic system.

- Information about workers' health collected to run a pension or insurance scheme should not be available to the employer unless this is necessary for the employer's role in administering the scheme.

3.1.5 Do not collect more information about workers' health than is necessary for the purpose(s) behind its collection.

Key points and possible actions

- Review any health questionnaires to ensure that only information that is really needed is collected.

- If commissioning a medical report on a sick employee, seek information on the worker's fitness for continued employment rather than medical details.

- Do not ask workers to consent to the disclosure of their entire general practitioner record as a matter of expediency. Only seek the disclosure of the whole record, or substantial parts of it, where this is genuinely necessary.

- If seeking a report from a worker's general practitioner or other medical practitioner who has been responsible for the care of the worker, ensure that you meet the requirements of the Access to Medical Reports Act 1988. This includes obtaining the worker's consent to your application for a report.

3.2 SICKNESS AND INJURY RECORDS

3.2.1 Where possible keep sickness and injury records separate from absence and accident records. Do not use sickness or injury records for a particular purpose when records of absence could be used instead.

Key points and possible actions.

- Review how sickness and accident records are currently kept.
- If necessary, change the way information on sickness and accidents is kept so that information on workers' health is not accessed when only information on absence or the circumstances of an accident at work is needed.
- Inform those accessing both sickness / injury and absence records of when it is and is not necessary to access the full sickness or injury record.

3.2.2 Ensure that the holding and use of sickness and injury records satisfies a sensitive data condition.

Key points and possible actions.

- Check current practices on the use of sickness and injury records against the sensitive data conditions in the Code.
- Take any remedial action necessary, including restricting the purposes for which records can be used and / or deleting records if no condition can be satisfied.
- Inform those handling sickness and injury records of any changes in procedures or practices.

See Supplementary Guidance Page 17 which explains more about the sensitive data conditions.

3.2.3 Only disclose information from sickness or injury records about an identifiable worker's illness, medical condition or injury where there is a legal obligation to do so, where it is necessary for legal proceedings or where the worker has given explicit consent to the disclosure

Key points and possible actions.

- Ensure that all those who deal with workers' sickness or injury records are aware of the circumstances in which there may be a legal obligation to disclose.

- Ensure, when appropriate, that written consent is obtained from the worker.

3.2.4 Do not make the sickness, injury or absence records of individual workers available to other workers unless it is necessary for them to do their jobs

Key points and possible actions.

- Managers can be provided with information about those who work for them in so far as this is necessary for them to carry out their managerial roles.

- No 'league tables' of individual records should be published.

- Ensure that managers are aware of the sensitive nature of sickness and injury records.

3.3 OCCUPATIONAL HEALTH SCHEMES.

This section gives good practice recommendations for employers with occupational health schemes. It does not provide detailed professional guidance to doctors, nurses and others involved in such schemes.

3.3.1 Ensure workers are aware of how information about their health will be used and who will have access to it.

Key points and possible actions

- Unless told otherwise workers are entitled to assume that information they give to a doctor, nurse or other health professional will be treated in confidence and not passed to others.

- Set out clearly to workers, preferably in writing, how information they supply in the context of an occupational health scheme will be used, who it might be made available to and why.

3.3.2 Do not compromise any confidentiality of communications between workers and health professionals in an occupational health service.

Key points and possible actions

- If workers are allowed to use telephone or e-mail for confidential communication with their occupational health service, do not compromise this confidentiality by monitoring the contents of these communications.

3.3.3 Act in a way that is consistent with the Guidance on Ethics for Occupational Physicians published by the Faculty of Occupational Medicine.

Key points and possible actions.

- Although this is guidance for occupational physicians rather than employers, it should give you a clear understanding of the legal and ethical constraints that apply to the exchange of information when working with occupational health professionals.

3.4 INFORMATION FROM MEDICAL EXAMINATION AND TESTING.

This subsection gives good practice recommendations specific to the collection and handling of information derived from medical examination and testing. The general recommendations in section 3.1 should also be taken into account.

Employers should bear in mind that obtaining a worker's consent or satisfying another sensitive data condition is not, on its own, sufficient to ensure data protection compliance. There is still an obligation to ensure that information obtained through medical examination is relevant, is accurate, is up to date and is kept secure.

See Supplementary Guidance page 17 for more Information on the Sensitive Data Conditions.

3.4.1 Where information obtained from medical testing is used to enforce the organisation's rules and standards make sure that the rules and standards are clearly set out in a policy which workers are aware of.

Key points and possible actions

- Ensure workers understand these rules and standards.
- Set out the circumstances in which medical testing may take place, the nature of the testing, how information obtained through testing will be used, and the safeguards that are in place for the workers that are subject to it.

3.4.2 Only obtain information through medical examination or testing of applicants or other potential workers at an appropriate point in the recruitment process, i.e. where there is a likelihood of appointing them. You must also be satisfied that the testing is a necessary and justified measure to:

- **Determine whether the potential worker is fit or likely to remain fit to carry out the job in question, or**
- **Meet any legal requirements for testing, or**
- **Determine the terms on which a potential worker is eligible to join a pension or insurance scheme.**

Key points and possible actions

- Record the business purpose for which examination or testing is to be introduced and the sensitive data condition that can be satisfied.

- Consider less intrusive ways of meeting the objectives, for example using a health questionnaire as an alternative to a medical examination or as a means to select those required to undergo a full examination.

- Only carry out a pre-employment medical examination or medical testing where there is a real likelihood that the individual will be appointed.

- Make it clear early on in the recruitment process that individuals may be subjected to medical examination or testing once there is a likelihood that they will be appointed.

3.4.3 Only obtain information through a medical examination or medical testing of current workers if the testing is part of a occupational health and safety programme that workers have a free choice to participate in, or you are satisfied that it is a necessary and justified measure to:

- **Prevent a significant risk to the health and safety of the worker, or others, or**

- **Determine a particular worker's fitness for carrying out his or her job, or**

- **Determine whether a worker is fit to return to work after a period of sickness absence, or when this might be the case, or**

- **Determine the worker's entitlement to health related benefits eg sick pay, or**

- **Prevent discrimination against workers on the grounds of disability or assess the need to make reasonable adjustments to the working environment, or**

- **Comply with other legal obligations.**

Key points and possible actions

- Record the business purpose for which the programme of examination or testing of workers is to be introduced and the sensitive data condition that can be satisfied.

- Establish and document who will be tested, what precisely are they being tested for, the frequency of testing, and the consequences of a positive or negative test.

- Consider less intrusive ways of meeting the employer's objectives, for example collecting information via a health questionnaire either as a first stage or as an alternative to a medical examination.

3.4.4 Do not obtain a sample covertly or use an existing sample, test result or other information obtained through a medical examination for a purpose other than that for which it was originally obtained.

Key points and possible actions

- Be clear about the purpose(s) for which any testing is being carried out and communicate this to workers.
- The covert obtaining of bodily samples for testing is most unlikely ever to be justified.
- If there is a wish to carry out a different test on an existing sample, this can only be done if the worker has been told about it and has freely consented.

3.4.5 Permanently delete information obtained in the course of medical examination or testing that is not relevant for the purpose(s) for which the examination or testing is undertaken.

Key points and possible actions

- Health information that is excessive, irrelevant or out of date should not be retained by an employer.
- If the retention of medical information is necessary only for the operation of an occupational health service, it should be kept in a confidential occupational health file.

3.5 INFORMATION FROM DRUG AND ALCOHOL TESTING.

This part of the Code gives good practice recommendations specific to the collection and handling of information derived from drug and alcohol testing. The recommendations in Sections 3.1 and 3.4 should also be taken into account.

3.5.1 Before obtaining information through drug or alcohol testing ensure that the benefits justify any adverse impact, unless the testing is required by law.

Key points and possible actions

- The collection of information through drug and alcohol testing is unlikely to be justified unless it is for health and safety reasons.
- Post-incident testing where there is a reasonable suspicion that drug or alcohol use is a factor is more likely to be justified than random testing.
- Given the intrusive nature of testing employers would be well advised to undertake and document an impact assessment

See Page 13 for information about how to carry out an impact assessment.

3.5.2 Minimise the amount of personal information obtained through drug and alcohol testing.

Key points and possible actions

- Only use drug or alcohol testing where it provides significantly better evidence of impairment than other less intrusive means.
- Use the least intrusive forms of testing practicable to deliver the benefits to the business that the testing is intended to bring.
- Tell workers what drugs they are being tested for.
- Base any testing on reliable scientific evidence of the effect of particular substances on workers.
- Limit testing to those substances and the extent of exposure that will have a significant bearing on the purpose(s) for which the testing is conducted.

3.5.3 Ensure the criteria used for selecting workers for testing are justified, properly documented, adhered to and are communicated to workers.

Key points and possible actions

- It is unfair and deceptive to lead workers to believe that testing is being carried out randomly if, in fact, other criteria are being used.
- If random testing is to be used, ensure that it is carried out in a genuinely random way.
- If other criteria are used to trigger testing, for example suspicion that a worker's performance is impaired as a result of drug or alcohol use, the employer should ensure workers are aware of the true criteria that are used.

3.5.4 Confine the obtaining of information through random testing to those workers who are employed to work in safety critical activities.

Key points and possible actions

- Collecting personal information by testing all workers in a business will not be justified if in fact it is only workers engaged in particular activities that pose a risk.
- Even in safety-critical businesses such as public transport or heavy industry, workers in different jobs will pose different safety risks. Therefore collecting information through the random testing of all workers will rarely be justified.

3.5.5 Gather information through testing designed to ensure safety at work rather than to reveal the illegal use of substances in a worker's private life.

Key points and possible actions

- Very few employers will be justified in testing to detect illegal use rather than on safety grounds. Testing to detect illegal use may, exceptionally, be justified where illegal use would:
  - breach the worker's contract of employment, conditions of employment or disciplinary rules, and
  - cause serious damage to the employer's business, e.g. by substantially undermining public confidence in the integrity of a law enforcement agency.

3.5.6 Ensure that workers are fully aware that drug or alcohol testing is taking place, and of the possible consequences of being tested.

Key points and possible actions

- Explain your drug or alcohol policy in a staff handbook.
- Explain the consequences for workers of breaching the policy.
- Ensure workers are aware of the blood-alcohol level at which they may be disciplined when being tested for alcohol.
- Do not conduct testing on samples collected without the worker's knowledge.

3.5.7 Ensure that information is only obtained through drug and alcohol testing that is;

- **of sufficient technical quality to support any decisions or opinions that are derived from it and,**
- **subject to rigorous integrity and quality control procedures and,**
- **conducted under the direction of, and positive test results interpreted by, a person who is suitably qualified and competent in the field of drug testing**.

Key points and possible actions

- use a professional service with qualified staff and that meets appropriate standards.
- ensure workers have access to a duplicate of any sample taken to enable them to have it independently analysed as a check on the accuracy of the employer's results.
- do not assume that the tests are infallible and be prepared to deal properly with disputes arising from their use.

3.6 INFORMATION FROM GENETIC TESTING.

Genetic testing has the potential to provide employers with information predictive of the likely future general health of workers or with information about their genetic susceptibility to occupational diseases. Genetic testing is, though, still under development and in most cases has an uncertain predictive value. It is rarely, if ever, used in the employment context. The Human Genetics Commission advises that employers should not demand that an individual take a genetic test as a condition of employment. It should therefore only be introduced after very careful consideration, if at all. This subsection supplements sub-sections 3.1 and 3.4.

3.6.1 Do not use genetic testing in an effort to obtain information that is predictive of a worker's future general health.

Key points and possible actions

- Obtaining information through genetic testing is too intrusive and the information's predictive value is insufficiently certain to be relied on to provide information about a worker's future health.

3.6.2 Do not insist that a worker discloses the results of a previous genetic test.

Key points and possible actions

- It is important that workers are not put off taking genetic tests that may be beneficial for their health care by the fear that they may have to disclose the results to a current or future employer.

- You can ask for information that is relevant to your health and safety or other legal duties but the provision of the information should be voluntary.

3.6.3 Only use genetic testing to obtain information where it is clear that a worker with a particular, detectable genetic condition is likely to pose a serious safety risk to others or where it is known that a specific working environment or practice might pose specific risks to workers with particular genetic variations.

Key points and possible actions

- Only seek information through genetic testing as a last resort, where:

- it is not practicable to make changes to the working environment or practices so as to reduce risks to all workers and
- it is the only reasonable method to obtain the required information.

- Inform the Human Genetics Commission of any proposals to use genetic testing for employment purposes.

3.6.4 If a genetic test is used to obtain information for employment purposes ensure that it is valid and is subject to assured levels of accuracy and reliability.

Key points and possible actions

- There should be scientific evidence that any genetic test is valid for the purpose for which it is used.

- Ensure the results of any test undertaken are always communicated to the person tested and professional advice is available.

- Ensure test results are carefully interpreted, taking account of how they might be affected by environmental conditions.

If you wish to contact us:

Information Commissioner,
Wycliffe House, Water Lane,
Cheshire, SK9 5AF

Telephone: 01625 545700
Fax: 01625 524510
E-mail@ico.gsi.gov.uk

Website: www.informationcommissioner.gov.uk