Scottish Executive

Health Department

NHS MEL (2000) 17

14 April 2000

Dear Colleague

DATA PROTECTION ACT 1998

Summary

1. The main provisions of the Data Protection Act 1998 came into force on 1 March 2000. This MEL highlights in the Annex the main implications for the NHSiS and the consequent action the NHSiS should take in order to comply with the Act. Data Protection is a reserved matter and this Act applies throughout the Kingdom. This MEL does not provide a complete description of the Act. Further information about the Act can be found on the Data Protection Commissioner's website at http:/www.dataprotection.gov.uk.

Background

2. The Data Protection Act 1998 is the main instrument for giving effect to the 1995 EC Directive on Data Protection. In broad summary, the Act sets out a number of data protection principles with which all organisations processing personal data (data controllers) must comply. Amongst other things, these regulate the fairness and lawfulness of the processing, the accuracy of the data and the purposes for which the data may be processed, the time for which the data may be retained and the need for security. These principles are set out in the Annex.

3. The presumption of a right to confidentiality continues to apply to patients' identifiable data. All NHSiS staff have a duty to maintain the confidentiality of personal health information and guidance on handling personal health information rests on the Code of Practice on the Confidentiality of Personal Health Information. NHSiS bodies should continue to have regard to the code which was issued to all staff in 1990. This Code will be revised and updated over the coming months to take account of the provisions of the new Act.

Addresses

For action
General Managers, Health Boards
General Manager, CSA
General Manager, State Hospital
Chief Executives, NHS Trusts
Chief Executive, Scottish Ambulance Service
Directors of Public Health, Health Boards
Medical Directors, NHS Trusts
Caldicott Guardians

For information
Chairmen, Health Boards and NHS Trusts
Those on Annex C

Enquiries to:

Miss Uriel Jamieson
Health Care Policy Division
2E (North)
St Andrew's House
EDINBURGH EH1 3DG

Tel: 0131-244 2397
Fax: 0131-244 2051

Further copies of this MEL may be obtained from

Lynsey Cooper
Health Care Policy Division
2E (North)
St Andrew's House
EDINBURGH EH1 3DG

Tel: 0131-244 2272
Fax: 0131-244 2051

E-mail:
Lynsey.Cooper@scotland.gov.uk

αβχδε αβχ α

Action

4. The following action will be necessary to ensure compliance with the Act:

- All staff dealing with personal information should be aware of the need for compliance with the Act and associated provisions, in particular those concerning the rights of data subjects (patients) in respect of their health records. In particular staff need ready access to the Data Protection (Subject Access Modification) (Health) Order 2000.

- The Data Protection Officer, or other person with responsibility for data protection matters should be aware of the detailed provisions of the Act and secondary legislation and of any subsequent guidance issued by the Scottish Executive Health Department and by the Data Protection Commissioner, and should ensure that the processing of personal data within the organisation is in compliance with the Act.

- Ensure that notification of processing of personal data is made to the Data Protection Commissioner in the required form, including the new requirement for general details of the organisation's security arrangements.

- Ensure that any arrangement to process personal data on behalf of the organisation is subject to a written contract which requires compliance with appropriate security and confidentiality arrangements.

5. Consultation is currently taking place on a Freedom of Information Bill, which will grant access to information held by a public body. It is anticipated that any application for personal information under such provisions would be treated as an application under the Data Protection Act. Further guidance on Freedom of Information will be issued in due course.

6. This MEL and annexes can be found in the publications section of the Scottish Health on the Web Website (SHOW), http://www.show.scot.nhs.uk. The Data Protection Act 1998 and subordinate legislation may be accessed through the Home Office website URL http://www.homeoffice.gov.uk/ccpd/dpsubleg.htm

Yours sincerely

KEVIN J WOODS
Director of Strategy and Performance Management

ANDREW FRASER
Deputy Chief Medical Officer

αβχδε αβχ α

Data Protection Commissioner

1. The title of the Data Protection Registrar is changed to Data Protection Commissioner (DPC). As now, data controllers will need to notify the DPC about certain particulars (previously referred to as registration) and, in addition will need to include some details of security measures before processing data.

2. Certain data protection processes may be likely to cause substantial damage or substantial distress to, or prejudice the rights and freedoms of, data subjects. Therefore certain processes specified by Order will be subject to the process of "prior checking" by the DPC before processing commences. This will not affect processing already being undertaken at the time the Act comes into force. Paragraphs 16-19 provide further details on notification and prior checking arrangements.

3. The DPC has the power to serve an enforcement notice on a data controller who is believed to be contravening the Act; failure to comply is an offence. Requests may also be made by, or on behalf, of a data subject affected by the processing of personal data to the DPC for an assessment as to whether the processing is in compliance with the Act. The DPC may then issue an "information notice" to a data controller requiring information to assist the assessment.

4. The DPC has a duty to promote good practice and may disseminate codes of good practice to this end. Such codes may either be prepared by the DPC or by a "trade association" (ie a body that represents data controllers, such as the GMC or the BMA). If submitted to the DPC for approval, the latter codes will be subject to consultation by the DPC as part of the determination of whether the code promotes good practice. Thus more than one code may exist in a particular sector.

Scope of the Act

5. The Act defines personal data as that which relates to a living individual who **can be identified**:

- from that data or;
- from that data and any other information which is in the possession of, or likely to come into the possession, the data controller.

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Data is defined as information which is:

- processed automatically or recorded with the intention to process automatically or;
- recorded as, or with the intention that it be, part of a manual "relevant filing system" which is further defined in the Act or;
- contained in a health, educational or social works services record.

αβχδε αβχ α

The definition of processing is wider than in the 1984 Act. It is defined as obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data and this includes:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

A health record for the purposes of the Act is one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of the individual.

Thus with the exception of anonymised information most if not all NHSiS information concerning patients, whether held electronically or on paper, will fall within the scope of the Act. The inclusion of manual or paper based records within the scope of the Act is one of the major changes from the 1984 Act.

Data Protection Principles

6. All processing of data to which the Act applies must comply with 8 principles. These are set out in Schedule 1 of the Act and are:

- 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.

- 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.
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- personal data shall be accurate and, where necessary, kept up to date.
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- personal data shall be processed in accordance with the rights of data subjects under this Act.
- 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.
- 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.

αβχδε αβχ α

Part II of Schedule 1 of the Act provides a more detailed interpretation of certain of these provisions which should be consulted as appropriate.

Schedule 2 conditions apply to the processing of all personal data. More stringent protection is provided for sensitive data about racial or ethnic origin, physical or mental health or condition and sexual life. Processing of such data must meet on of the conditions of not only Schedule 2 but also Schedule 3 of the Act. One of these conditions is that the processing is necessary for "medical purposes" which is not defined exhaustively but includes preventative medicine, medical diagnosis, medical research, provision of care and treatment and the management of health care services.

Access to Health Records Act 1990

7. The provisions of the Access to Health Records Act 1990 have been subsumed within the 1998 Data Protection Act with the exception of section 3(f) of the 1990 Act relating to access to a deceased person's records. In addition, the 1998 Act makes provision for data subjects to have access to all health records not just that part made after 1 November 1991. This will apply from the date of the implementation of the Act. It should be noted that deceased persons records remain subject to an access restriction prior to 1 November 1991.

Data Protection (Subject Access Modification) (Health) Order 2000

8. This Order is similar but not identical to the Data Protection (Subject Access Modification) Health Order 1987. Its main effect is to create an exemption from the right of subject access to health data where giving access would cause serious harm to the health of a data subject or another individual. Where the data controller is not a health professional, he may not grant or withhold subject access without first having consulted a doctor, who should normally be the individual's own doctor.

αβχδε αβχ α

Data Protection (Miscellaneous Subject Access Exemptions) Order 2000

9. This Order also mirrors existing provisions. It provides subject access exemptions for certain information where disclosure is prohibited or restricted by the statutes specified in the Schedule. This covers information about human fertilisation and embryology, adoption records, information about children's special education needs, parental order records, and information provided by the principal reporter in children's hearings in Scotland.

10. More detailed guidance on rights of access to health records will be distributed shortly.

Responding to access requests and fees

11. A request for access must be made in writing, and no reason need be given. Subject to any applicable exemption, the applicant must be given a copy of the information and, where the data is not readily intelligible, an explanation (eg of abbreviations or medical terminology). Data controllers may not charge for the explanation, but can charge a fee for the application and copying charges.

Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000

12. Regulations on subject access fees have been agreed up until 23 October 2001 and are publicly available on the HMSO website. The regulations provide that a maximum fee of £50 can be charged for access to health records for a transitional period running until 24 October 2001.

Social Work Records

13. Separate guidance on the Data Protection Act 1998 is being prepared for Social Work Agencies. This will be issued in due course. The relevant provisions of the DPA for social work services will be introduced during the first transitional period (commencement of the Act until 23 October 2001). NHS Trusts and social work services will need to have appropriate procedures in place where joint records are held. While both organisations will be required to notify separately – as both are data controllers in their own right – either organisation can provide access to the joint record. Therefore the data subject should only have to apply to the NHSiS Trust or social work services for access to their records. NHSiS Trusts and social work services will need to have procedures in place to inform the data subject that the data are held jointly, that access can be provided through either organisation, and to inform each other that access has been given.

αβχδε αβχ α

14. It should be noted that where information held by a social work agency contains details provided by a health professional, the agency must not disclose that health information without first consulting the "appropriate health professional" (AHP). This would normally be the person responsible for the data subject's current clinical care in connection with the matters to which the information relates, for example a GP or psychiatrist. The final decision regarding access rests with the social work department after taking full account of the views of the AHP about whether or not disclosure of the information is likely to harm the physical or mental health of the data subject (Article 5(2) of the Data Protection (Subject Access Modification) (Health) Order 2000 refers). Its main effect is to create a subject access exemption where giving access would prejudice social work because of the serious harm caused to the health of the data subject or another individual.

Overseas transfer of information

15. If data is to be transferred overseas, then the eighth data protection principle must be observed: Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (The EEA consists of the EU member states including Iceland, Norway and Liechtenstein. It does not include Switzerland and the USA).

Notification and Security

16. The Act prohibits processing of automated data and manual data subject to prior assessment unless there is an entry for the data controller in the register maintained by the DPC. However, since data subjects can require the registrable particulars in respect of manual data that has not been notified, it is advisable to effect voluntary notification in respect of such data.

17. Entry to the register is by notification to the DPC. The notification must, as did the 1984 Act, include certain information specified in section 16 of the Act. The categories of information required are similar, but not identical to, that required under the 1984 Act.

18. A new requirement is that notification must include a general description of the measures taken to comply with the 7th principle, concerning security (see Annex 1, section A). A statement that the organisation complies with guidance on security best practice issued by the Scottish Executive Health Department may meet this requirement.

19. Further guidance on notification is available from the DPC.

αβχδε αβχ α

Transitional Provisions

20. These are set out in Schedule 8 to the Act. The following paragraph gives an outline of the transitional provisions:

Manual Records

20.1 During the period from commencement of the Act until 23 October 2001, manual social work services or health records are exempt from its provisions except for sections 7 and 12A (ie access and correction rights of data subject). All other manual files which were held immediately before 24 October 1998, will be exempt from all relevant parts of the Act.

20.2 Between 24 October 2001 and 23 October 2007, more limited exemptions apply (to manual data held immediately before 24 October 1998 and, in any event, to all manual data in social work services or health records). The exemptions cover the first data protection principle (but not the obligation to give basic information to the data subject contained in Schedule 1 Part II) the second to fifth data principles (see Annex 1, section A) and sections 12A and 14 of the Act (rectification rights etc). Further exemptions apply to data that is processed only for historical research purposes.

Automated Data

20.3 Provided automated data was held before 24 October 1998, it is exempt during the first transitional period (commencement of the Act until 23 October 2001) for most parts of the Act except certain obligations in section 7 (to inform the data subject of the processing and where lawful communicate the information consisting the data by way of a copy pursuant to section 8) section 14 (rectification etc) as well as the general obligation to ensure that processing is fair. Further exemptions apply to data that is processed only for historical research purposes.

General

20.4 Manual files (other than social work services or health records) and automated data created after 24 October 1998 will immediately become subject to all of the provisions of the Act.

21. From 24 October 2001, the full regime will apply to all automated data and from 24 October 2007, the full regime will also apply to all manual files covered by the Act (whenever collated or created).

αβχδε αβχ α

ANNEX B

SOURCES OF FURTHER INFORMATION

1. Principle 7 of the 1998 Data Protection Act states "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".

2. The Information and Statistics Division have produced "Data Protection Act 1998 – An Action Plan for the NHSiS" (http://www.show.nhs.uk/publications/dp/dpaction.pdf) to assist the NHSiS in implementing the new Act.

3. The other areas of activity on implementation will include:

- Developing a Security Culture via training and awareness events and the provision of training materials, increasingly via electronic media.

- Contributing to the development and promulgation of national policy, standards and best practice for Security and Data Protection in the NHSiS.

- Assisting the NHSiS to manage security risks through advisory services and an Incident Reporting Scheme.

4. Other ways of promulgating advice will include:

- News bulletins on SHOW (http://www.show.nhs.uk/showmain/sh00.htm).

- A library of Frequently Asked Questions.

- Action points and checklists.

- Protect newsletters produced quarterly by the NHSiS Data Protection Adviser.

- "NHSiS Data Protection Manual".

- Presentations at national forums eg NHSiS ITSO forums.

αβχδε αβχ α

Further information can be obtained from:

Uriel Jamieson
Health Care Policy Division
NHS Management Executive
St Andrew's House
Regent Road
EDINBURGH
EH1 3DG

Tel: 0131 244 2392
Fax: 0131 244 2051
E-mail: Uriel.Jamieson@scotland.gov.uk

Patricia Ruddy
NHSiS Data Protection Adviser
ISD Scotland
Trinity Park House
South Trinity Road
EDINBURGH
EH5 3SQ

Tel: 0131 551 8359
Fax: 0131 551 8495
E-mail: Patricia.Ruddy@isd.csa.scot.nhs.uk

John Bigham
IS/IT Security Consultant
Information and Systems Support Group
Trinity Park House
South Trinity Road
EDINBURGH
EH5 3SQ

Tel: 0131 551 8377
Fax: 0131 551 8495
E-mail: John.Bigham@isd.csa.scot.nhs.uk

Office of the Data Protection Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545575
Fax: 01625 524510
E-mail: data@wycliffe.demon.co.uk

αβχδε αβχ α

ANNEX C

Accounts Commission
Association of Optometrists
British Dental Association
British Medical Association, Scottish Council
BUPA
Chartered Society of Physiotherapy
Clinical Standards Board for Scotland
College of Optometrists
Conference of Colleges and Faculties in Scotland
Convention of Scottish Local Authorities
Council for Professions Supplementary to Medicine
Deans of Dental Schools
Deans of the Faculties of Medicine
Deans of Postgraduate Medical Education
Director, Cancer Registration
Directors of Education
Director of Public Health Group
Director, Scottish Association of Health Councils
Directors of Social Work
Executive Director, SCPMDE
Faculty of Advocates
Health Board Directors of Nursing (Scotland) Group
Health Education Board for Scotland
Health Service Commissioner (Scotland)
Joint Committee for Postgraduate Training of GPs
Local Research Ethics Committee
Marie Curie Hospices
Medical and Dental Defence Union of Scotland
Mental Welfare Commission for Scotland
Multi Centre Research Ethics Committee
National Board for Nursing, Midwifery and Health Visiting in Scotland
National Dental Advisory Committee
National Health Service Central Register (Scotland)
National Nursing, Midwifery and Health Visiting Advisory Committee
National Paramedic Advisory Committee
National Pharmaceutical Advisory Committee
Office for Public Health in Scotland
Practice Managers Association
Practice Nurse Association

αβχδε αβχ α

Royal College of Anaesthetists
Royal College of General Practitioners, Scottish Council
Royal College of Midwives
Royal College of Nursing
Royal College of Obstetricians and Gynaecologists (Scottish Executive)
Royal College of Ophthalmologists
Royal College of Optometrists
Royal College of Paediatrics and Child Health (Scottish Committee)
Royal College of Physicians of Edinburgh
Royal College of Physicians and Surgeons, Glasgow
Royal College of Psychiatrists, Scottish Office
Royal College of Pathologists (Scottish Affairs Committee)
Royal College of Radiologists
Royal College of Surgeons of Edinburgh
Royal Pharmaceutical Society for Great Britain (Scottish Department)
SAC Faculty of Public Health Medicine
Scottish Association of Health Councils
Scottish Association of Medical Directors
Scottish Association for Mental Health
Scottish Centre for Infection and Environmental Health
Scottish Chief Administrative Pharmaceutical Group
Scottish Committee of Optometrists
Scottish Consumer Council
Scottish Council for Postgraduate Medical and Dental Education
Scottish Courts Administration
Scottish Dental Practice Board
Scottish General Practice Committee
Scottish Health Visitors Association
Scottish Independent Acute Sector Management Group
Scottish Independent Hospital Association
Scottish Joint Consultants Committee
Scottish Law Commission
Scottish Medical and Scientific Advisory Committee
Scottish National Blood Transfusion Service
Scottish Partnership Agency for Palliative and Cancer Care
Scottish Prison Service
Scottish Trade Union Council
Scottish Health Advisory Service
The Law Society of Scotland
Trust Directors of Nursing (Scotland) Group
UKCC
UNISON

αβχδε αβχ α