
The Data Protection Act 1998

An Action Plan for the NHSiS

Information & Statistics Division
Common Services Agency
National Health Service in Scotland

December 1999

Contents

Summary 3

Introduction 4

ACTION PLAN (Table) 5

Management action 6

Registration (Notification) 7

Manual records 8

The Data Protection Principles

- First Principle 9
- Second Principle 11
- Third Principle 11
- Fourth Principle 12
- Fifth Principle 12
- Sixth Principle 12
- Seventh Principle 13
- Eighth Principle 14

Individual's Rights 15

Transitional provisions 16

Appendix: Information sources 17

Summary

This paper presents an action plan to help NHSiS organisations move towards compliance with the data protection legislation (both current and forthcoming). The target audience includes Information Managers/Data Protection Officers and Caldicott Guardians in Health Boards and NHSiS Trusts and those who are charged with data protection responsibilities in Primary Care. A reasonable level of knowledge about existing data protection legislation is assumed, but basic information concerning the operation of the current Acts and other relevant material is to be found in the Appendix on Information Sources.

All action should be directed towards achieving the principle aim of the Data Protection Act 1998, strengthening the individual's right to privacy with respect to the processing of personal data. The legislation is intended to ensure that any processing of personal data (including that done by the NHSiS for its legitimate purposes) is done in accordance with the rights of individuals.

A table of 36 action points is presented and these are expanded further under a series of topic headings.

This action plan has been prepared by ISD Scotland, in association with the Office of the Data Protection Registrar, the Scottish Executive Health Department and staff working within the NHSiS. It is based on a paper produced by the NHS Information Authority, Birmingham, with permission.

If you have any comments about this paper, or wish to seek further advice please contact:

The NHSiS Data Protection Adviser

ISD Scotland
Trinity Park House
South Trinity Road
Edinburgh EH5 3SQ

Tel (Help Desk): 0131 551 8359
Fax: 0131 551 1392

Introduction

The replacement of the *Data Protection Act 1984* by the *Data Protection Act 1998* has been long awaited. Delays in drafting the secondary legislation, necessary for the implementation of the Act, mean that it will not come into force until 1 March 2000.

The delay has created uncertainty and caused confusion amongst those working in all sectors. There is increasing concern about what action should, and could, be done. In the health service much of the work generated by the *Caldicott Report* will also be appropriate to the new data protection act.

Many NHSiS organisations will have begun work, led by Caldicott Guardians and supporting staff, that can be built upon to prepare for the Data Protection Act. There is a good deal of synergy between the Caldicott work programme and that required under data protection legislation, and there is clearly an opportunity for work to be prioritised in order to satisfy the requirements of both. Although personal data, defined in data protection terms, is broader than patient identifiable information referred to by Caldicott, both are concerned with computerised and manual records. The management audit required of organisations to support the Caldicott programme and the related improvement plans should serve as a major “building block” for assessing compliance with most of the data protection principles. Clearly, compliance with the law must be seen as a priority, and NHSiS organisations should be aware that the Data Protection Registrar/Commissioner has been increasingly critical of NHS performance in this area and has demonstrated that she may take action in response to a complaint or a request for assessment.

Whilst it is not yet possible for anyone (including the Data Protection Registrar/Commissioner) to provide comprehensive practical advice on all aspects of compliance with the new Act, some preparatory action is possible: much assessment and planning can begin now. This plan is intended to be a framework, outlining actions that should be taken and issues that need to be addressed by an NHSiS organisation. It will assist organisations in being better prepared to meet the requirements of the 1998 Data Protection Act. Some of the actions can be achieved relatively quickly; but much will require a longer term approach. Please note that this plan does not purport to be comprehensive, and following the advice offered does not, in itself, give any guarantee of compliance with the 1998 Act. Also, it intentionally describes only *what* actions are required, not *how* they should be carried out. Further detailed guidance and training will become available from a variety of sources.

The plan takes the form of 36 action points which are listed in the table below, then described in more detail on the following pages. For ease of reference, they are set out under various headings. A list of useful information sources is appended. It is intended that this plan should be read in conjunction with the publications referred to therein.

Action Plan

Management		1	Identify/appoint a Data Protection lead person
		2	Keep up-to-date on Data Protection developments
		3	Promote staff awareness
		4	Train staff
Registration (Notification)		5	Review existing registrations
		6	Check that registration covers the entire organisation
		7	Conduct data audit
		8	Identify 'new processing' (i.e. from 24.10.98)
		9	Reduce register entries to one
Manual Records		10	Audit manual record systems
		11	Include manual records in compliance plans
Data Protection Principles	- First Principle	12	Review all processing operations to ensure legitimacy
		13	Test Caldicott protocols for compliance
		14	Inform data subjects of processing operations
		15	Consider other measures required for legitimacy
	- Second Principle	16	Review purposes and processing for compatibility
		17	Ensure disclosures are properly handled
	- Third Principle	18	Ensure good data management practices are applied
		19	Ensure compliance with existing guidelines
- Fourth Principle	20	Ensure accuracy of data	
	21	Make provision for data subject's comments	
- Fifth Principle	22	Review procedures for retention and disposal	
	23	Ensure compliance with retention requirements	
- Sixth Principle	24	Ensure data subjects' rights can be respected	
- Seventh Principle	25	Review data security	
	26	Ensure good data management practice	
	27	Address relevant organisational issues	
	28	Follow best practice guidelines on security	
	29	Test contingency arrangements	
	30	Address obligations regarding data processors	
- Eighth Principle	31	Conduct audit of overseas transfers	
	32	Review processing outside the EEA	
	33	Ensure written contracts are in place	
Individual's Rights		34	Review/amend subject access arrangements
		35	Provide details of data processing operations
		36	Address issues relating to automated decision taking

Management action

Action that can be taken now includes:

1. Identify/appoint a person to manage data protection compliance within your organisation.
2. Maintain current awareness of developments in data protection (see Appendix - Information Sources).
3. Promote a general awareness campaign for staff, patients and the public about data protection and the way in which it is being implemented within the organisation.
4. Ensure that staff are adequately trained and instructed - to include induction and regular updating sessions with properly documented working instructions.

Registration (Notification)

Notes

Registration must give a clear description of the nature of the processing of personal data by an organisation (details of systems are not required). Organisations registering should aim for transparency and simplicity. Currently, NHSiS organisations often have many register entries; under the 1998 Act an organisation will only be permitted one notification.

Important

All NHSiS organisations will need to notify and all will be required to adhere to the Data Protection Principles.

Actions

5. Review existing registration(s) and ensure they are up to date.
6. Check that the data processing activities of all parts of your organisation are registered; (for Health Boards, in conjunction with their PCTs, this will include reminding General Medical and Dental Practitioners, Pharmacists and Optometrists of their legal obligations under the Data Protection Act).
7. Conduct an audit of both manual and computerised patient/personal data and data flows and ensure that these are accurately reflected in the register entry/ies. Note the overlap with the Caldicott work programme for 1999/2000.
8. Ensure that any new processing which commenced on or after 24th October 1998 can be clearly identified as it will have to be done in accordance with the requirements of the new Act as soon as it is implemented. (For further information regarding new processing see “*The Data Protection Act 1998: An Introduction*”, Chapter 6).
9. Reduce multiple register entries to one as renewal dates arise.

Manual records

Note

Under the Data Protection Act 1998 most manual records containing personal data are covered by data protection legislation for the first time.

Actions

10. Identify which of your manual systems for handling personal information fall within the scope of the 1998 Data Protection Act. Remember that manual systems (e.g. card indices) will cover more than just health records. Personnel, occupational health, finance, contractors, suppliers, volunteers and other data in the form of a 'relevant filing system' are to be covered. (For further information regarding the definition of 'relevant filing system' see "*The Data Protection Act 1998: An Introduction*", Chapter 2).
11. The Data Protection Principles now cover manual records and must be applied appropriately.

The Data Protection Principles

The Data Protection Act 1998 contains further interpretation of each of the Principles which are stated below.

1 The First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- *at least one of the conditions in Schedule 2 is met, and*
- *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

Notes

“Processing” under the new Act “means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data . . . “ This is very much broader than the previous definition and covers all processes from the initial obtaining of the data right through to its disposal or destruction.

The general view of what constitutes fair and lawful processing is that:

- the common law of confidentiality is complied with
- the data subject was not misled or deceived into giving the data
- the data subject is given basic information about who will process the data and for what purpose(s)
- in the case of health data (described in the Act as sensitive personal data) one of the conditions in each of Schedules 2 and 3 to the Act is satisfied.

The conditions in Schedule 2 and Schedule 3 are **additional** tests, not a replacement for lawfulness and fairness. For further information see “*The Data Protection Act 1998: An Introduction*”, Chapter 3: 1 - 1.5.

Even where Schedules 2 and 3 are satisfied, other laws must be complied with and where sensitive patient information is to be processed particular regard must be paid to the common law duty of confidence. This requires that unless there is a statutory requirement or a sufficiently robust public interest justification, patient information should only be used for purposes that the patient has been informed about and has consented to either implicitly or explicitly.

The common law, which is based upon an evolving body of case law, is open to differing interpretations. Scottish Executive Health Department guidance is that it need not be construed so as to disadvantage patients, that many NHSiS activities are in the public interest and that where patients have been effectively informed of the intended uses of information and do not object, their consent can be implied. However, given the possibility of conflicting interpretations of the common law, wherever practicable, explicit consent is clearly preferable. In the Data Protection Registrar/Commissioner’s view, the normal basis for processing personal data about an individual’s health should be consent.

For further interpretation of the first principle refer to the “fair processing code”, described in “*The Data Protection Act 1998: An Introduction*”, Chapter 3: 1.9 - 1.12.

Actions

12. Review all existing processing operations against the “fair processing code” to ensure legitimacy.
13. Ensure that protocols for sharing patient identifiable information, being developed as part of the Caldicott work programme, comply with the requirements of the Data Protection Act 1998.
14. Ensure that data subjects are properly informed about the identity of the data controller and the purpose(s) for which data will be processed. A proforma (or similar) may help demonstrate compliance with this requirement in order to “bridge the gap” between the data subject’s expectation regarding processing and what takes place in reality.
15. Consider what other measures are needed by your organisation to fulfil the requirement for legitimacy.

2 The Second Principle

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.

Notes

Simply registering the purpose(s) will not be sufficient to achieve compliance with this Principle. The concept of a lawful purpose is particularly relevant to public sector organisations as the activities they may legitimately engage in are generally set out in law. The fact that the purpose(s) must be specified is intended to promote transparency in the processing and to limit the data controller's processing of personal data to the specified purpose(s). The requirement for further processing to be compatible mirrors the principle of common law that confidential information obtained for one purpose cannot be used for some other purpose without the consent of the subject (unless there is an overriding public interest).

An additional test of compatibility will have to be satisfied (either in a notice to the data subject as part of the fair processing information, or in a notification given to the Commissioner - provisions for this are not yet in place).

Actions

16. Ensure that the purposes for which you obtain personal data are both specified and lawful and that all processing is adequately covered by them (see *"The Data Protection Act 1998: An Introduction"*, Chapter 3: 2).
17. Ensure that disclosure(s) are compatible with the purpose(s) for which the personal data were obtained. Furthermore, ensure that those to whom personal data may be disclosed will not use them for purposes incompatible with the purposes for which they were originally obtained. (Note the overlap with the protocols required as part of the Caldicott work programme for 1999/2000).

3 The Third Principle

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

Actions

18. Audits should already be routinely conducted as part of good data management practice (Note, also, the overlap with the Caldicott work programme for 1999/2000. You will also wish to refer to *"Guidance for the Retention and Destruction of Health Records"*, NHS MEL(1993)152 and *"Scottish hospital service: destruction of hospital records"*, SHM58/60 and its accompanying schedule).
19. Note the existence of health service and professional guidelines regarding the taking and making of records and the need for action to ensure professionals adhere to them.

4 The Fourth Principle

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

Note

Data are inaccurate if they are incorrect or misleading as to any matter of fact.

Actions

20. Take all reasonable steps to ensure the accuracy of the data (Note, also, the overlap with the Caldicott work programme for 1999/2000).
21. Make provision for recording a data subject's comments about the accuracy of their personal data.

5 The Fifth Principle

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

Actions

22. Review procedures for retention and disposal of records. (Note, also, the overlap with the Caldicott work programme for 1999/2000. You will also wish to refer to “*Guidance for the Retention and Destruction of Health Records*”, NHS MEL(1993)152 and “*Scottish hospital service: destruction of hospital records*”, SHM58/60 and its accompanying schedule).
23. Review compliance with legal requirements and established guidelines for retention periods. (Note the guidance contained in “*Guidance for the Retention and Destruction of Health Records*”, NHS MEL(1993)152 and “*Scottish hospital service: destruction of hospital records*”, SHM58/60 and its accompanying schedule).

6 The Sixth Principle

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

Notes

Contraventions of this Principle include:

- failure to supply information following a subject access request
- failure to prevent processing notified as likely to cause damage or distress
- failure to comply with a notice to prevent processing for direct marketing
- failure to comply with a notice in relation to automated decision taking.

See Chapter 3:6 of “*The Data Protection Act 1998: An Introduction*” for additional information.

See also the section on Individuals' Rights below.

Action

24. Ensure procedures are in place to satisfy the rights of data subjects.

7 The Seventh Principle

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.

Notes

See Chapter 3:7 of *“The Data Protection Act 1998: An Introduction”* for further guidance.

The baseline requirements for ensuring security and confidentiality in NHSiS organisations are set out in the *“NHSiS IT Security Policy”* and *“Manual”*. Local IT Security Policies and manuals will also apply.

Particular obligations are placed upon data controllers regarding data processors. Written contracts will be required.

Actions

25. Review all aspects of data security - manual and computerised. The security measures in place for manual records (e.g. hospital case notes, General Practice Lloyd George envelopes) require particular consideration as they have not previously been covered by legal data security requirements.
26. Ensure that good data management practices are in place. (Note, *“Guidance for the Retention and Destruction of Health Records”*, NHS MEL(1993)152 and *“Scottish hospital service: destruction of hospital records”*, SHM58/60 and its accompanying schedule).
27. Address the organisational issues involved e.g. appointment of Caldicott Guardian and Information Security Officer, procedures for staff recruitment, wording of contracts of employment, training (induction and ongoing) and protocols for granting access to personal data. (Note overlap with Caldicott recommendations.)
28. Follow current best practice guidelines on information and IT security.
29. Test your capability to respond to a breakdown or other serious contingency in your operations which could affect the handling of all forms of personal data.
30. Enter into written contracts with all data processors that undertake work for your organisation. Ensure that strict quality, security and data protection compliance mechanisms and inspection procedures are agreed and enforced. Remember to include those who process manually held information (e.g. microfilming or paper disposal) as well as those who undertake automated data processing.

8 The Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), 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.

Notes

The EEA consists of the 15 European Union Member States plus Iceland, Norway and Liechtenstein. Special consideration will be required for processing carried out elsewhere.

It is the responsibility of the Data Controller to ensure that appropriate protection is in place.

Actions

31. Conduct an audit of data transfers overseas.
32. Review all processing by companies based outside the EEA.
33. Contracts between the person/organisation exporting the data and the overseas recipient will be needed to meet the requirements of the new legislation (but note the derogations, i.e. circumstances in which the eighth principle does not apply to a transfer). See “*The Data Protection Act 1998: An Introduction*”, Chapter 3:8 for further details.

Remember

Under The Data Protection Act 1998 the Eight Data Protection Principles apply to ALL data controllers (whether they are registered or not!).

Individuals' Rights

Notes

The Act gives seven rights to individuals in respect of their own personal data held by others. They are:

- right of subject access
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
- right to take action to rectify, block, erase or destroy inaccurate data
- right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

See the *Data Protection Act 1998* (Part II) and “*The Data Protection Act 1998: An Introduction*” (Chapter 4) for fuller details.

The *Access to Health Records Act 1990* is to be superseded (apart from the sections dealing with access to information about the deceased) and data subjects' rights of access to their health records will then be governed by the *Data Protection Act 1998*. This will apply from the date of implementation of the new Act (i.e. 1 March 2000). Note that data subjects will have access rights to all records irrespective of when they were created.

Actions

34. Review your existing arrangements for providing subject access and amend as necessary to meet the requirements of the new legislation. Additional guidance on subject access, replacing that relating to the *Access to Health Records Act 1990*, will be available shortly.
35. Ensure, when responding to subject access requests, that individuals are given information about the processing of their data as well as a copy of the data.
36. Consider whether any automated decision taking occurs within your organisation (e.g. evaluating an individual's performance at work, reliability or conduct). If such processing constitutes the sole basis for making the decision, the data subject must be informed about the logic involved in the automated decision taking when a subject access request is made.

Transitional provisions

The 1998 Act introduces a range of new measures and requirements into the data protection arena. In addition, some exemptions and exclusions of the earlier legislation are removed. To ease the transition from the old to the new, some transitional arrangements are specified in the Act. (For further details see “*The Data Protection Act 1998: An Introduction*”, Chapter 6).

The provisions are somewhat complex. The advice of the Data Protection Registrar is that it will be easier for an organisation to try to comply with all the provisions of the new Act as soon as practicable rather than to attempt to determine which processing is eligible for transitional relief and which is not. Each NHSiS organisation should put in place mechanisms for ensuring that it can comply with the Data Protection Act 1998 as quickly as is practicable.

The 36 point action plan above indicates how much planning and work is required.

Our strong recommendation and key message is:

Begin your preparations and actions now !

Appendix: Information sources

Publications

The EU Data Protection Directive (95/46/EC) <http://www2.echo.lu/legal/en/dataprot/dataprot.html>

Published by The Stationery Office Limited

The Data Protection Act 1998 <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

Published by the Office of the Data Protection Registrar

The Data Protection Act 1998: An Introduction. <http://www.dataprotection.gov.uk/eurotalk.htm>

The Guidelines: The Data Protection Act 1984, Fourth Series, September 1997. <http://www.open.gov.uk/dpr/guide.htm>

Published by the Scottish Executive Health Department

Guidance for the Retention and Destruction of Health Records. NHS MEL(1993)152

Scottish hospital service: destruction of hospital records. SHM58/60 and its accompanying schedule.

Play IT Safe. A practical guide to Information Security for everyone working in General Practice. Issued 1999.

NHSiS Data Protection Manual relates to the 1984 Data Protection Act (out of print).

Protecting and Using Patient Information: A Manual for Caldicott Guardians. Issued March 1999. <http://www.show.scot.nhs.uk/>

Published by the Information Systems Support Group (ISSG)

The NHSiS IT Security Policy (1993) and Manual (1994).

Published by the British Standards Institution

Guide to the Practical Implementation of the Data Protection Act 1998. (DISC PD 0012 1999). <http://www.bsi.org.uk/pd12>

Other web sites

Scottish Executive Health Department <http://www.show.scot.nhs.uk/dtc>

Home Office <http://www.homeoffice.gov.uk>

The Stationery Office <http://www.hmso.gov.uk>

Scottish Health on the Web <http://www.show.scot.nhs.uk>

PROTEC (Data Protection Newsletter for the NHSiS) <http://www.show.scot.nhs.uk/publications/dp/index.htm>

Addresses

Office of the Data Protection Registrar

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Tel: 01625 545700

Fax: 01625 524510

Email: data@wycliffe.demon.co.uk

Web site: <http://www.dataprotection.gov.uk>

British Standards Institution

389 Chiswick High Road
London W4 4AL

Tel: 0181 996 9000

Fax: 0181 996 7448

Web site: <http://www.bsi.org.uk>

Scottish Executive Health Department

St Andrew's House
Regent Road
Edinburgh EH1 3DG

Tel: 0131 244 2428

Fax: 0131 244 2051

The Stationery Office Limited (Bookshop)

71 Lothian Road
Edinburgh EH3 9AZ

Tel: 0131 228 4181

NHSiS Data Protection Adviser

ISD Scotland
Trinity Park House
South Trinity Road
Edinburgh EH5 3SQ

Tel: 0131 551 8359

Fax: 0131 551 1392

Email: John.Pelham@isd.csa.scot.nhs.uk