



THE SCOTTISH OFFICE

National Health Service in Scotland Management Executive

NHS
MEL (1992)42

St. Andrew's House
Edinburgh EH1 3DE

Telephone 031-244
Fax 031-244 2683

Dear Colleague

SAFEGUARDING THE CONFIDENTIALITY OF PERSONAL DATA ASSOCIATED WITH CONTRACTS

Summary

1. This letter reviews arrangements for safeguarding the confidentiality of personal data following our experience of the contracting process to date and its widening in Scotland on 1 April 1992.

Background

2. Annexed is the document "Guidance for the secure handling of confidential information in the contracting environment". It builds on and supersedes SOHHD/DGM (1991)39, extends the guidance given at page 81 of the Procedural Manual on Contracting for Hospital & Community Services, accords with the Code of Practice on Confidentiality of Personal Health Information and is informed by the terms of the CRAG Working Group on Access to Named Data (the Weir Report).
3. The guidance identifies key principles and requires that mechanisms to protect patient confidentiality are established and operated within all purchaser (excluding GP Fundholders who are bound by their professional ethical code) and provider Units involved in the sending, receipt, storage and use of person identifiable information acquired in the contracting process. These mechanisms develop the concept of the "safe haven" which was introduced in the 1991 DGM.
4. Our aim is to ensure that access to patient identifiable information in contracting is strictly controlled on need to know basis. In particular it is essential to minimise the risk of

7 August 1992

Addressees

For action:

General Managers,
Health Boards

General Manager,
Common Services Agency

General Manager, State
Hospital

Chief Executives, NHS
Trusts

For information:

General Manager,
Health Education Board
for Scotland

To be copied to Unit
General Managers

Enquiries to:

Mr C B Knox
Director of Information
Services
Keith House
2 Redheughs Rigg
South Gyle
EDINBURGH

Tel: 031-317-2250

Fax: 031-317-8112

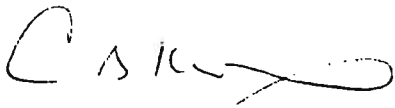
SCOTTISH HEALTH SERVICE COMMON SERVICES AGENCY TRIP HOUSE LIBRARY	
O: <i>let</i>	
A: <i>12/10/92</i>	<i>2969</i>
Date /	Price /

staff members and others having accidental sight of information to which they are not entitled as part of their legitimate NHS activities, and to limit the scope and opportunity for deliberate unauthorised access to such information.

5. The guidance is intended to maintain the trust with which patients disclose information to their doctors and to enable the contracting process to proceed effectively. We have a duty to preserve the confidentiality of patient identifiable information and the NHS in Scotland has a proud record in this respect. I know I will have your full co-operation in maintaining that.

Action

6. Recipients are asked to ensure that all appropriate staff are aware of and follow the guidance annexed.
7. This circular should be copied to Unit General Managers for action.



C B Knox
Director of Information Services

N.H.S. in Scotland Management Executive

Guidance for the Handling of
Confidential Personal Health
Information in the Contracting
Environment

Directorate of Information Services

GUIDANCE FOR THE HANDLING OF CONFIDENTIAL PERSONAL HEALTH INFORMATION IN THE CONTRACTING ENVIRONMENT

SCOPE

1. This guidance covers all person identifiable information acquired and exchanged in the contracting process.

1.1 It therefore applies to:-

- (a) Information exchanged between purchaser and provider and between providers in support of contract management.
- (b) Information supplied to support the notification/authorisation of extra-contractual referrals (ECRs).
- (c) The transmission and receipt of Contract Minimum Data Sets (CMDS) where this is necessary.
- (d) Information supplied to support contracts between the Health Service and local Authorities and Voluntary Agencies.

1.2 It does not apply to GP Fundholders

REFERENCES

NHS Circular No. 1990(GEN)22 : Confidentiality of Personal Health Information : A Code of Practice (7 June 1990)

CRAG Working Group Report on Access to Named Data (the Weir Report)

BACKGROUND

2. The availability and ease of access to computer terminals and computers has greatly increased the risk of accidental or deliberate illegitimate access to confidential information held in the computer. This is a general problem extending far beyond contracting issues. In this more general context, it is useful to distinguish between named data, identifiable data and anonymised data, viz.
 - (a) named data implies that clinical or other NHS data is linked to the patient's name and maybe his/her address;
 - (b) identifiable data has no associated name or address but has a number or key such as CHI number and maybe postal code which allows the data to be linked to the patient's name and address;
 - (c) anonymised data has had all markers of identity removed - name, address and identifying number - and there is no possibility of linkage either with the patient as a person or of events occurring in the same patient.

3. Information is collected by the NHS in Scotland about their patients for a number of essential purposes:-
 - (a) clinical care
 - (b) patient administration
 - (c) medical record management
 - (d) teaching and training
 - (e) clinical audit
 - (f) medical audit
 - (g) disciplinary proceedings
 - (h) research
 - (i) monitoring
 - performance
 - quality of patient care
 - service
 - (j) assessment of health care need
 - (k) epidemiological studies
 - (l) management of contracting
 - (m) financial audit

Nor should names ever appear on an invoice. In both cases a provider reference number should be used in place of names to provide a means of making enquiries and linking with other information. Wherever possible the CHI number coupled with the provider institution number should be used. Where CHI number is not available the local PAS number or case reference number with the provider institution number will serve in its place;

- (c) In setting contracts purchasers and providers must agree upon the information that is to be provided by the provider to the purchaser in support of contract management. Anonymised and, preferably, aggregated information should be used. Names should only be included as part of that supporting information where it is agreed to be essential to the proper management of the contract. In every individual case, separate consideration must be given to the need for use of the name. Specifically the agreement of the purchasers CAMO will be required to the inclusion of name. It is expected that name will not be a necessary item in information supporting block or cost and volume contracts. In cost per case contracts the CHI number or the local PAS number or case reference number with the provider institution number must be used in preference to names;
- (d) When purchasers outside of Scotland require name as part of a contract minimum data set (for example in respect of ECRs) this should not be withheld but procedures for dispatch should accord with the transmission of named data detailed later in this guidance.
- (e) For the purposes of health care needs assessment and epidemiological research named data sets will continue to be available to purchasers and others through the established SMR return files for which confidentiality procedures are well established;
- (f) Contract management systems established by providers may contain named records derived from SMR return files. Separation of identifying information from clinical information will be achieved by password control procedures agreed by the CAMO or senior designated doctor. The intention of these controls will be to limit the disclosure of information to those with clear and agreed need to know.
- (g) It is recognised that auditors may have access to named data but the procedures for such access should be agreed by the CAMO or senior designated doctor and should be based on "need to know" with adequate separation of duties within audit staff designed to avoid unnecessary disclosure.

4. Whatever the purpose for which data are collected key principles attach to the collection, storage and subsequent retrieval of that data. These principles are referred to in the Code of Practice on Confidentiality of Personal Health Information and were at the heart of the work of the CRAG Working Group. They are also directly relevant to our responsibilities under the Data Protection Act 1984. They are:-
- (a) Fair Obtaining : the patient should be aware of each purpose for which the information is to be used. (Data Protection Principle 1 and Code of Practice para 7)
 - (b) Need to know : defined as "... should only be disclosed in connection with the purposes of health care and social welfare to those who would be unable to provide effective treatment and care without that information". (Code of Practice para 1.2)
 - (c) Minimum disclosure necessary for the purpose: under the Data Protection Act data shall be held for one or more specified and lawful purposes, shall not be used or disclosed in any manner incompatible with these purposes, shall be adequate, relevant and not excessive in relation to the purposes and shall not be kept longer than is necessary for those purposes. (Data Protection Principles 2,3,4 and 6 and Code of Practice para 12)
 - (d) Safeguards to ensure that damage or distress to the subject of the information is avoided and that anonymity is secured where necessary and particularly in any published material. (Code of Practice para 12)
5. All persons involved in the handling of health information in the NHS have a legal duty of confidence towards patients, reinforced through their contract of employment (or equivalent formal relationships with the NHS). A breach of patient confidentiality resulting from a breach of agreed procedures has always been and will remain a serious disciplinary matter.
6. The protection of patient confidentiality is a clear duty when designing, developing, using and managing all the information systems required by the NHS in Scotland.
7. The guidance sets out the principles and management arrangements which must be adopted by providers and purchasers for handling confidential information in the contracting process.

PRINCIPLES

8. As a general policy, it is intended that information in computer systems and relating to patients should be held in an identifiable but not named form. Linkage with name and address will be tightly controlled and should occur only where clinical care of individual patients is being delivered. This policy is to be implemented in all NHS in Scotland computer systems - clinical as well as administrative. Implementation of this policy is a major task. It will require substantial planning and will take time to achieve. The detailed implications will be considered in a later circular.
9. In accordance with the Code of Practice (para 7) information leaflets or patient handbooks should contain reference to the circumstances in which personal health information should be disclosed. Such leaflets or handbooks should, in future, include reference to the use of such information for financial purposes. The precise wording of the statement which should be used is currently under discussion with the Data Protection Registrar and will be issued in due course. Hospitals etc should ensure that the wording in this statement is used, unaltered, for this purpose.
10. The need to know principle must be strictly enforced. Access to patient identifiable information will be confined to those who would be unable to provide effective treatment or care without that access or whose access has been explicitly authorised by the CAMO, senior designated doctor or his nominated representative. The CAMO, in granting such authorisation, should have regard to the terms of this guidance which establishes a range of measures to allow the contracting process to proceed effectively and ensures the protection of confidentiality.
11. To achieve the minimum disclosure necessary for the purpose a number of measures are required:-
 - (a) Each purchaser and provider must establish a "safe haven", a concept which was introduced in SOHH/DGM(1991)39. The term "safe haven" refers to both a physical location and to an agreed set of administrative arrangements for ensuring the safety and secure handling of confidential patient identifiable information. Further information about the management arrangements for these safe havens is given later in this guidance;
 - (b) The Management Executive is clear that identifiable information should be passed from one safe haven to another only where this is absolutely necessary and it's security should be ensured during transfer. Accordingly it has been decided that it is not necessary for names to be passed from a provider to a purchaser when giving notification of or seeking authorisation for an ECR.

12. Safeguards to ensure that damage or distress to the subject of the information is avoided and that anonymity is secured where necessary and particularly in any published material will include the measures described above and will include a range of detailed measures described in the following guidance. In particular existing procedures for handling highly sensitive information such as that relating to psychiatric conditions, gynaecological problems and sexually transmitted diseases should be continued as at present and any development must ensure at least as high a level of security and confidentiality.

MANAGEMENT ARRANGEMENTS

13. Each purchaser and provider must establish a "safe haven" for ensuring the safety and confidential handling of person identifiable information required and used in the contracting process. This includes having a single designated contact point.
14. All information exchanged between providers and purchasers as part of the contracting process must be between "safe haven" contact points.
15. The policies and procedures which govern the safe haven must be approved by the General Manager and by the Chief Administrative Medical Officer (CAMO) or, for NHS Trusts, by the Chief Executive and senior designated doctor.
 - 15.1 The General Manager or, for NHS Trusts, the Chief Executive, carries final responsibility for the adequacy of "safe haven" procedures and for ensuring the implementation of this guidance;
 - 15.2 The Code of Practice on the Confidentiality of Personal Health Information states that the CAMO or his nominated deputy has responsibility for the confidentiality, security and access to personal health information held by a Health Board and should be regarded as a source of advice on all aspects of disclosure. For an NHS Trust this responsibility rests with the senior designated doctor.
 - 15.3 The officer who is assigned responsibility for the day to day operation, administration and management of the "safe haven" should have clear authority to ensure that agreed procedures are effective and efficient.
16. All members of staff should be aware of the existence of the "safe haven" and the policies and procedures surrounding it.
 - 16.1 This should include instructions on how to handle incorrectly directed inquiries or information and identification of the personnel and building areas which constitute the physical safe haven.
17. All switchboard operators should know the name and extension number of the safe haven contact and introduce callers requesting this number as "caller for safe haven" to guard against having dialled the wrong extension number.
 - 17.1 Ideally the switchboard should be able to release other safe haven information such as full address of the safe haven, fax number and electronic mail details; however, there will always be the option of passing the caller to the safe haven contact person.

PROCEDURES

18. The policies and procedures which govern the safe haven must be fully and clearly documented.
 - 18.1 The full document should be agreed at the highest level of the organisation and be capable of being shown to outside bodies or individuals as necessary.
 - 18.2 The procedures must be comprehensive and cover:-
 - (a) Management arrangements.
 - (b) Receipt of information.
 - (c) Physical location of offices and devices for receiving information.
 - (d) People responsible for managing the information.
 - (e) People with access to the information in their work.
 - (f) Procedures for handling information.
 - (g) Disclosure of information.
 - (h) Storage of paper information.
 - (i) Use of computer systems.
 - (j) Archiving and destruction of information.
 - 18.3 Important elements of procedure are:-
 - (a) Identification of the detailed steps in each fundamental activity carried out in the safe haven;
 - (b) To substitute the use of patient name and full address with the CHI number and post code at the earliest practical opportunity, ie. move from named data to anonymised data in terms of para 2 of this guidance;
 - (c) Computer held data must comply with the provisions of the Data Protection Act 1984. In particular, care must be taken not to hold data items, particularly patient name, which are unnecessary for the system's purposes;
 - (d) Identification of which individuals can perform a given step in a given activity. Individuals may be identified by name or job title;
 - (e) Inclusion of an appropriate audit trail to track the movement of all confidential information used to support contracts;

- (f) Identification of each level of authority and responsibility applicable to safe haven procedures, from responsibility for executing a task correctly to responsibility for the procedures themselves;
- (g) Identification of those individuals authorised to disclose confidential information other than as part of the retrieving process and to indicate clearly the source of the authority given to them;
- (h) Photocopying of confidential information should be avoided as far as possible;
- (i) When not in use, paper-based information should always be kept within folders, envelopes and other containers which prevent sight of the paper and locked securely away;
- (j) Movement of confidential information beyond the safe haven physical area should be strongly discouraged. For example, to work at home or attend external meetings, a formal authorisation and logging process should be required with written justification for each removal from the safe haven. In these circumstances the materials should ideally be transported in a locked brief case or other secure device;
- (k) Confidential information should not be retained either on paper or on magnetic or electronic form any longer than necessary, or to comply with statutory requirements.

19. In practice, the safe haven procedures are likely to be centred on the contracts departments. This means the validation of invoices, handling of queries arising, and authorisation for payment will take place in safe haven areas.

20. The actual process of making payments once authorised does not require the use of confidential information and can take place outside safe haven areas.

20.1 It should be established practice to separate this aspect of accounts from the validation and querying of invoices which must take place within the safe haven.

20.2 It is recognised that there will be a period of transition where an ECR has been approved or notification accepted against a patient's name.

SECURITY OF PHYSICAL LOCATIONS

21. One of the most important features of a safe haven is the physical security of information. This applies in particular to paper based data and to stand alone computer systems. It is important to ensure that people who enter the physical safe haven area, but who do not have authority to access confidential information, are prevented from doing so by physical measures, primarily key locks. The fundamental objective is to restrict physical access to those with appropriate authority in the safe haven.
22. The safe haven should ideally occupy a clearly identifiable part of the organisation's premises which should ideally be contiguous.
 - 22.1 This reduces the need to transport confidential information between areas. Where this is impracticable, because the work is dispersed over a number of physically separate locations, safe haven procedures should apply to each location.
 - 22.2 In particular, there must be one clearly identified safe have contact point through which all incoming and outgoing communications will pass.
23. Access to the safe haven area should normally be restricted.
 - 23.1 This will prevent conversations being overheard, paper - or screen-based confidential information, particularly that which is in current use, being read. The clear priority in this respect is to ensure that members of the public and visitors to the premises do not gain access to these areas. It is good practice to hold any meetings involving staff who are not in the safe haven physically outside the safe haven.
24. Where possible the safe haven area should have only one "normal" entry point.
 - 24.1 There should be a reception/enquiries office clearly visible which contains no confidential information (although the staff may have certain levels of authorisation for accessing confidential information). This could be the point to which post is delivered (but preferably not opened).
25. Archived material (paper or magnetic) should be kept under two levels of lock.
 - 25.1 The first lock gains access to the filing room; the second lock allows use of a given cabinet. Since filing, and particularly archiving, are comprehensive sources of confidential information and are generally infrequently used, the number of people having easy access could be more restricted than usual.

26. Offices in the safe haven area should normally be locked when not in use.

26.1 This simplifies the need to repeatedly lock away information on short trips away from the office. However, all confidential information should be left covered so that it cannot be read through any window, including glass door.

CONTROLLING ACCESS TO INFORMATION

People

27. There should be named individuals responsible for managing the information in the safe haven. All other staff should only be allowed the level of access to the information required by his or her job.
- 27.1 An important part of restricting the access to confidential information is to define clearly those people who do have the authority to access confidential information. Each organisation should identify, for each member of staff, the level of authority with regard to access to safe havens and confidential information. The number and the nature of the levels of authority will depend on local policies and procedures.
- 27.2 In determining each individual's level of authority, an organisation should actively seek to:-
- (a) minimise the use of confidential information;
 - (b) minimise the number of people with access to confidential information.
- This involves isolating the business activities which involve use of confidential information and using a limited set of people to conduct them.
- 27.3 Key points to observe are:-
- (a) temporary staff should not normally be employed within the safe haven;
 - (b) the need for clerical and secretarial staff to be involved in the administration of confidential information must be acknowledged. Staff's suitability for employment within the safe haven should depend on their personal attributes, not their grade;
 - (c) when identifying staff roles and numbers, appropriate allowance must be made for cover during absence for any reason. The most obvious person to deputise for a given individual is their immediate superior; however, this is not a hard and fast rule.
28. Wherever possible organisations should separate responsibilities on a need to know basis so as to limit the authority of any one individual to have access to all aspects of a named patient's records.
29. It will be clear that the procedures for handling confidential information and the authority for access must be carefully co-ordinated with the physical security measures in place and affects, in particular, the issuing of keys to staff.

COMMUNICATIONS

30. Each organisation should ensure that other organisations can easily and confidently direct patient identifiable information to its intended safe haven.
 - 30.1 Information about purchaser's safe haven contact point may be needed by a wide variety of providers based anywhere in Great Britain. The feasibility of producing a national directory of safe havens containing postal, and e-mail address and telephone and fax numbers of all purchasers is under consideration.
 - 30.2 All providers must issue information about their safe haven contact point to the purchasers with whom they are currently in contact or whom they contact for the first time. Each purchaser will then compile a directory of provider safe haven information.
31. A change in safe haven information will be rare, but has serious implications for possible accidental breaches of confidentiality. Wherever possible, such changes should be planned well in advance and preferably aligned with the new financial year and corresponding reconfirmation of safe haven details. In any case, every practicable step must be taken to ensure that materials sent using the old information will not fall into the wrong hands. The GPO should be asked to redirect mail for at least two years; BT or Mercury should be asked not to re-allocate phone numbers (where it has not been possible to re-use them). Similar precautions should be taken when the change is purely internal.

POST

32. All mail must be marked "SAFE HAVEN - confidential : return to sender if undelivered" at the top left-hand corner. The address of the sender's safe haven contact point must be stated.
 - 32.1 The post room should have clear instructions to direct any mail marked "safe haven" to the safe haven contact point. Where there is any doubt about whether an incoming item of post is intended for the safe haven; it should be directed to the safe haven in the first instance.
 - 32.2 The full address for safe haven information should not include a person's name since this clouds the key issue: the document must be delivered to a safe haven or not at all. This will also avoid difficulties arising if a member of staff has left the organisation's employment.

33. Except in the circumstances referred to in para 33.2 when posting invoices and supporting named data sets, they should be sent together in the same envelope but providers must ensure that the named data set is enclosed in a separate sealed envelope within the common cover and marked for the attention of the CAMO or senior designated doctor.

33.1 Providers should adopt the practice of sealing the named data set in an envelope, marking the envelope for the attention of the CAMO or senior designated doctor, and attaching to it an authorisation to raise the invoice (bearing hospital number and treatment details), before passing it to their finance department. The invoice can then be attached to the sealed envelope and the two documents sent together to the purchaser's safe haven.

33.2 When invoices and associated named data sets are posted separately because to do otherwise would cause the invoice to be delayed beyond the timescale allowed for invoicing, they must still be sent to the safe haven.

FAX

34. It is imperative that the safe haven fax machine is placed in a secure location.

34.1 No named data should be sent by fax. If it is essential, clinical information can be sent with a suitable identifier and the name and address and identifier sent by post.

34.2 The room housing the fax machine must be locked whenever unattended. If the office is in general use, consideration must be given to ensuring that visitors are unable to read, accidentally or otherwise, faxes which are arriving or have recently arrived.

34.3 While it is critical to have the fax machine which is used for confidential information located in the safe haven area, it could still be the only fax machine in use by the organisation. In that case the safe haven staff will simply forward any faxes not intended for their area.

34.4 One problem is faxes arriving outside normal hours which could be seen by cleaners or other personnel. Options include a blanket ban on transmissions outside office hours, switching machines off over night if they are not secured and locking machines (while switched on) into a cupboard.

34.5 A further option involved the use of a computer to receive and store faxed data; the information cannot be extracted without a password.

35. Measures must be taken to minimise the risk of misdialling.
- 35.1 One of the most important risks with fax machines is mis-dialling, although most models show the number dialled. This can lead to faxes not arriving at all or arriving in an unintended location. In the latter case, there are serious implications if non-coded confidential information is on the fax.
- 35.2 Best practice involves always checking the safe haven fax number before dialling; never dial from memory. Valid sources would include a locally compiled safe haven directory or a national directory, but not a general directory; alternatively a telephone call to the safe haven should be used.
- 35.3 It is good practice to identify frequently used numbers and program these into a fax machine "memory dial" facility; equally computer dialling facilities may be used where available. However, numbers must be tested in conjunction with a telephone call before using them for confidential information. Furthermore, the use of "memory dial" codes should be limited to safe haven numbers, this will prevent code mis-dialling having serious consequences.
- 35.4 It is good practice to always seek confirmation from the intended recipient that the FAX has been received.

TELEPHONE

36. It is important to establish the types of information which may be received over the telephone and the circumstances in which they are received.
- 36.1 Common examples currently include a purchaser asking a hospital for a patient's name and the purchaser then discussing the case with the patient's General Medical Practitioner. Also some providers telephone ECR requests.
- 36.2 Where information is supplementing existing data, it is important to consider where it may be recorded. For example, it would be undesirable to write free text information on a piece of paper intended to be limited to code information. It may be appropriate for organisations to consider introducing standard paper forms to record information commonly received over the telephone.

37. Disclosure of information by telephone carries risks associated with speaking to the wrong person.

37.1 The following guidance should be followed:-

- (a) Always confirm the identity of the other party of the safe haven contact from the required organisation. Dial-back arrangements based on published phone numbers and caller's name could be considered, especially for uncommon requests.
- (b) Ensure that the correct patient has been identified using at least two pieces of information, such as name and date of birth.
- (c) The discloser should ensure that they know the reason why the other party requires the information.

38. In terms of addressing electronic mail, the guidance applied to postal addresses and fax numbers should be followed as appropriate to local circumstances.