Director-General Health & Social Care and
Chief Executive NHS Scotland
Derek Feeley

The Scottish Government

Dear Colleague

SAFEGUARDING THE CONFIDENTIALITY OF PERSONAL DATA PROCESSED BY THIRD PARTY CONTRACTORS

CEL 25 (2011)

November 2011

Summary

1. This circular provides revised guidance for the secure handling of person-identifiable information which is accessible to, or may be handled by, third party contractors. It supersedes NHS MEL (1992) 14, NHS MEL (1992) 42, and NHS MEL (1994) 100.

Background

2. The appropriate handling of person-identifiable information is vital to maintaining public trust and confidence in our healthcare services. The aim of this guidance is to ensure that all access to, and handling of, person-identifiable information by contractors is properly regulated under a set of clearly understood principles and contractual requirements. These will accord with the wider NHSScotland approach to Information Governance set out in the NHSScotland Information Assurance Strategy. These principles and contractual requirements are set out in Annexes 1 and 2 respectively.

Action

3. All Health Boards, Special Health Boards, and the Common Services Agency (referred to in this circular, including Annex 1, as "Boards") are asked to ensure all appropriate staff are aware of and follow the guidance set out in Annexes 1 and 2.

4. Boards should only select contractors who provide adequate assurances regarding the safeguards they use to protect person-identifiable information.

Addresses

For action
Chief Executives
Caldicott Guardians

For information
Information Governance Leads
eHealth Leads

Enquiries to:

eHealth Information Assurance Team
Scottish Government
Room BR.13
St Andrew's House
EDINBURGH EH1 3DG

Tel: 0131-244 2351
E-mail:ehealthinformationassurance@scotland.gsi.gov.uk

Further copies of this CEL can be downloaded from:

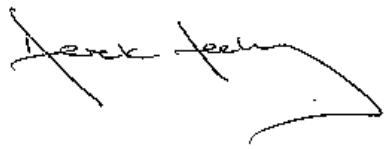
http://www.show.scot.nhs.uk/

5. This circular should be routinely used as a reference point when Boards are entering into contracts which may give rise to the possibility that a contractor may have access to, or be required to handle or "process", person-identifiable information held or controlled by that Board. The guidance pertains to new contracts, or where changes are being made to existing contracts that still have a substantial period to run.

6. Consideration should be given to incorporating the guidance outlined in Annex 1 into a Data Processing Agreement between the Board and the contractor.

7. Contractors should be obliged, as a minimum, to comply with the requirements detailed in Annex 2. This can be achieved by incorporating (by reference) the requirements detailed in Annex 2 into contracts between Boards and their contractors, or by agreeing contract terms that adequately deal with those requirements. If less formal contracting arrangements are in place, Boards could, for example, reference Annex 2 of this circular in their purchase order terms, or letters of appointment.

Yours sincerely



DEREK FEELEY
Director-General Health & Social Care and Chief Executive NHS Scotland

St Andrew's House, Regent Road, Edinburgh EH1 3DG
www.scotland.gov.uk

ANNEX 1

GUIDANCE FOR THE HANDLING OF PERSON-IDENTIFIABLE DATA INVOLVED IN CONTRACTS

SCOPE

1. This guidance covers all person-identifiable information accessed, acquired, held, exchanged, destroyed and otherwise "processed" (as such term is defined in the Data Protection Act 1998) by a third party contractor in the course of performing services for a Board, or in connection with preparatory and/or contractual arrangements relating to those services.

BACKGROUND

2. NHSScotland handles an increasing volume and complexity of person-identifiable information. Legislation such as the Data Protection Act 1998, the Human Rights Act 1998, and the Freedom of Information (Scotland) Act 2002, as well as the common law of confidentiality, provide the legal framework for the confidential and secure handling of person-identifiable information. In addition, guidance such as the NHSScotland Records Management Code of Practice, the NHSScotland IT Security Policy, the Scottish Government Identity Management and Privacy Principles, the NHSScotland Code of Practice on Protecting Patient Confidentiality, and the Scottish Government's Information Assurance Strategy, seek to promote best practice and quality standards in connection with working with person-identifiable information. It is essential that both the legal framework and all applicable guidance are adhered to when Boards use third party contractors to deliver services.

PRINCIPLES

3. A set of high level principles need to be adhered to, to ensure that person-identifiable information is handled in a safe and secure manner. These are set out in the following sections.

CONTRACTOR OBLIGATIONS

4. Contractors should be obliged, by being required to agree to contractual provisions at least equivalent to those detailed in Annex 2 to this circular, to comply with the various obligations detailed in Annex 2.

St Andrew's House, Regent Road, Edinburgh EH1 3DG
www.scotland.gov.uk

PROCEDURES AND MANAGEMENT ARRANGEMENTS

5. Underpinning the obligations set out in Annex 2, Boards should, prior to a contractor being in a position to **access and/or handle** person-identifiable information in respect of which the Board has legal responsibilities, also seek to develop and agree, with each contractor:

    a. a clear set of policies and procedures for the handling and processing of person-identifiable information;

    b. the scope and type of person-identifiable information that may be accessible as part of the contract. Minimum datasets should be agreed;

    c. a set of rules and protocols for the access to, and handling of, person-identifiable information as part of each contract. These should follow NHSScotland procedures as set out in the NHSScotland Records Management Code of Practice, the NHSScotland IT Security Policy, the eHealth Mobile Data Protection Standard, and the NHSScotland Code of Practice on Protecting Patient Confidentiality and should also be consistent with the Scottish Government Identity Management and Privacy Principles and the Scottish Government's Information Assurance Strategy. These rules and protocols will cover access to information and systems (access being for the duration of the contract only), and may include procedures for the withdrawal of access, and the return or deletion (at the Board's discretion) of all person-identifiable information on completion or termination of the contract.

6. Boards and contractors should establish and agree specified communications and access channels for the safe handling of person-identifiable information, including management arrangements.

7. All relevant Board and contractor staff, including reception/call-handling staff, should be made aware of these policies and procedures, with appropriate training provided. Boards should ensure that all relevant Board and Contractor staff are fully aware of the data storage capabilities of all equipment used in the delivery or receipt of services, including the fact that person-identifiable data may be stored on medical instruments and devices.

SECURITY AND COMMUNICATIONS

8. When communicating person-identifiable information, Boards should ensure that their own staff and contractors adhere to the Board's data handling arrangements, including any requirements or best practice relating to the anonymisation of data wherever feasible or appropriate. In particular:

St Andrew's House, Regent Road, Edinburgh EH1 3DG
www.scotland.gov.uk

a. Postal Mail

It is important to establish the types of information which may be received by post and the circumstances under which they would be received. The Board's guidance and procedures for the secure handling of postal mail should be followed by the contractor at all times, with processes agreed and documented as part of the terms of the contract;

b. Fax

No person-identifiable information should be sent by fax. Faxing is not a secure method of transmitting information, and its use should be actively discouraged.

Where it is considered absolutely necessary, fax machines should be sited appropriately within a secure area to avoid demands for access that could lead to the compromise of person-identifiable information. The Board's guidance and procedures for the secure handling of fax transmissions should be followed by the contractor at all times, with processes agreed and documented as part of the terms of the contract;

c. Telephone

It is important to establish the types of information which may be received over the telephone and the circumstances under which they would be received. Particular reference should be made to the appropriate usage of mobile and smartphones. The Board's guidance and procedures for the secure handling of telephone calls should be followed by the contractor at all times, with processes agreed and documented as part of the terms of the contract; and

d. Email and Electronic Transfer

Official NHS email accounts must be used (i.e. with NHS.net or NHS.uk) and board policies consulted before sending person-identifiable information via email to colleagues and partners outside the Board. This is because technical security, which includes encryption, varies depending on where the email is being sent and the sensitivity level of the information. The Board's guidance and procedures for the secure handling and transfer of electronic data should be followed by the Contractor at all times, with processes agreed and documented as part of the terms of the contract.

9. In line with the eHealth Mobile Data Protection Standard, person-identifiable information shall not be stored on mobile devices including laptops, USB memory sticks, PDAs, Blackberries or any other mobile device or media such as smart phones, CD or DVD, except when specifically authorised after a risk assessment of the necessary business case.

In some cases storing patient information on a mobile device may be unavoidable for the completion of work duties. Such cases shall:

- be subject to appropriate risk assessment and approval by the local IT security officer;
- meet the security requirements set out in the eHealth Mobile Data Protection Standard; and
- be approved by a Caldicott Guardian.

St Andrew's House, Regent Road, Edinburgh EH1 3DG
www.scotland.gov.uk

ANNEX 2

CONTRACTOR OBLIGATIONS

1. Contractor:

    a. agrees that, in respect of all "person-identifiable information" (such term meaning the same as "personal data", as defined in the Data Protection Act 1998) accessed by it, provided to it, and "processed" (such term being as defined in the Data Protection Act 1998) by it for the Health Board/Special Health Board (or the Common Services Agency, as the case may be) (the "Contract Purchaser") with which it has entered into the contract into which these terms are incorporated ("the "Contract") (such person-identifiable information being referred to below as "Contract Personal Data"), other than where otherwise specified by the Contract Purchaser, it is acting as a "Data Processor" in respect of Contract Personal Data for which the Contract Purchaser is "Data Controller" (such terms being as defined in the Data Protection Act 1998);

    b. undertakes (on its own behalf and on behalf of third party suppliers engaged by it):

        i. to act and procure that third party suppliers act only on the instruction of the Contract Purchaser in respect of Contract Personal Data;

        ii. to implement adequate technical and organisational measures (in light of the nature of the processing to be undertaken in relation to the Contract Personal Data) to protect the integrity of Contract Personal Data;

        iii. to not allow Contract Personal Data to be accessed by, or sent to, parties outside the EEA (unless expressly required or permitted to do so by the Contract Purchaser);

        iv. to comply in all respects with the Data Protection Act 1998, and to act in a manner which ensures that the Contract Purchaser complies with its obligations under the Data Protection Act 1998 as Data Controller in respect of Contract Personal Data;

    c. undertakes (on its own behalf and on behalf of all third party suppliers) to treat Contract Personal Data with which it deals in accordance with the provisions and principles of the Data Protection Act 1998 and to ensure only those of its staff who require to access Contract Personal Data in the performance of their duties under the Contract are able to do so, and that such staff are appropriately trained and vetted to ensure their reliability;

    d. shall only access person-identifiable information which is directly relevant to the effective execution by it of the terms of the Contract;

e. shall fully participate in any audit and monitoring activity associated with its appropriate usage of Contract Personal Data provided or generated under the terms of the Contract;

f. shall discuss and seek to reach agreement with the Contract Purchaser in relation to the scope and type of Contract Personal Data that may be accessible as part of the Contract. Minimum datasets should be agreed;

g. shall discuss and seek to reach agreement with the Contract Purchaser in relation to a clearly understood and mutually agreed set of access rules and protocols for the handling of Contract Personal Data as part of the Contract. These should follow NHSScotland procedures as set out in the NHSScotland Records Management Code of Practice, the NHSScotland IT Security Policy, the eHealth Mobile Data Protection Standard and the NHSScotland Code of Practice on Protecting Patient Confidentiality, and should also be consistent with the Scottish Government Identity Management and Privacy Principles and the Scottish Government's Information Assurance Strategy. These rules and protocols will cover access to information and systems for the duration of the Contract, and may include procedures for the withdrawal of access and the return or deletion (at the Contract Purchaser's discretion) of all person-identifiable information on completion or termination of the Contract;

h. return all Contract Personal Data to the Contract Purchaser on demand and on expiry of the Contract or, if requested to do so by the Contract Purchaser, shall securely destroy all Contract Personal Data when no longer required.

2. Contractor shall not, during and after the term of the Contract:

a. use any Contract Personal Data other than as directed by the Contract Purchaser;

b. use any Contract Personal Data for its own direct or indirect benefit, or the direct or indirect benefit of any third party, except that the Contractor may use Contract Personal Data to the extent necessary to perform its duties and obligations, or to enforce its rights, under the Contract;

c. seek to gain commercial advantage from its access to Contract Personal Data;

d. disclose any Contract Personal Data to third parties, other than as required by the terms of the Contract or as required by a court or other competent authority.

3. Contractor shall comply, and shall at all times act in such a manner to assist the Contract Purchaser to comply, with the following:

    a. the Data Protection Act 1998, and all codes and guidance issued pursuant thereto;

    b. the Human Rights Act 1998;

    c. the Common Law Duty of Confidentiality;

    d. NHSScotland Records Management Code of Practice, a copy of which is available on request from the Contract Purchaser;

    e. NHSScotland IT Security Policy, a copy of which is available on request from the Contract Purchaser;

    f. eHealth Mobile Data Protection Standard, a copy of which is available on request from the Contract Purchaser;

    g. NHSScotland Code of Practice on Protecting Patient Confidentiality, a copy of which is available on request from the Contract Purchaser;

    h. the Scottish Government Identity Management and Privacy Principles a copy of which is available on request from the Contract Purchaser;

    i. the Scottish Government's Information Assurance Strategy a copy of which is available on request from the Contract Purchaser;

    j. where written consent has been provided by the Contract Purchaser to the transfer of person-identifiable data outside the European Economic Area (EEA), the European Commission model clauses relating to the transfer of personal data outside the EEA, as advocated by the Information Commissioner's Office (and as updated or amended from time to time), such clauses being incorporated into the Contract by reference; and

    k. the Contract Purchaser's guidance and procedures in relation to communications by: post; fax; phone, email and other electronic transfers of data.