Caldicott policy

Issue sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSACG001c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td>S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review CG Policy\Current and Final</td>
</tr>
<tr>
<td>Title</td>
<td>NHS Business Services Authority Caldicott Policy</td>
</tr>
<tr>
<td>Author</td>
<td>Gordon Wanless</td>
</tr>
<tr>
<td>Issued to</td>
<td>All NHSBSA staff</td>
</tr>
<tr>
<td>Reason issued</td>
<td>For information / action</td>
</tr>
<tr>
<td>Last reviewed</td>
<td>17 March 2016</td>
</tr>
</tbody>
</table>

Revision details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial release</td>
<td>30.05.2007</td>
<td>-</td>
<td>IGSG</td>
<td>-</td>
</tr>
<tr>
<td>a</td>
<td>08.07.2008</td>
<td>Gordon Wanless</td>
<td>IGSG</td>
<td>Changed “HSG (96)18 The Protection &amp; Use of Patient Information” to be “Confidentiality: NHS Code of Practice”, along with associated explanatory text</td>
</tr>
<tr>
<td>b</td>
<td>01.07.2009</td>
<td>Gordon Wanless</td>
<td>IGSG</td>
<td>Changed role name for CG and widened policy to cover person-identifiable information and not just patient identifiable information</td>
</tr>
<tr>
<td>c</td>
<td>16.01.2014</td>
<td>Gordon Wanless</td>
<td>IGSG</td>
<td>Changed role name for CG</td>
</tr>
<tr>
<td>d</td>
<td>16.04.2015</td>
<td>Chris Gooday</td>
<td>IGSG</td>
<td>Annual Review</td>
</tr>
<tr>
<td>e</td>
<td>17.03.2016</td>
<td>Richa Bhuttar / Gordon Wanless</td>
<td>IGSG</td>
<td>Add in changes for Caldicott 2</td>
</tr>
</tbody>
</table>
Contents

1. Introduction
2. Policy statement
3. Principles
4. Scope of this policy
5. Associated legislation
6. Training, policies and procedures
7. Advice and guidance
8. Validity of this policy

Appendix

A Data Protection Act 1998 – Data protection principles
B Caldicott Guardian job description

1. Introduction

1.1 In December 1997 the Caldicott Report identified weaknesses in the way NHS organisations handled confidential patient identifiable information.

1.2 One of the recommendations stated that all NHS organisations appoint a Caldicott Guardian to ensure patient identifiable information is kept secure. Caldicott Guardians are senior members of staff, preferably at board level.

1.3 The NHSBSA executive director board role that has been appointed as the Caldicott Guardian is currently the Director of Service Delivery. The job description for the Caldicott Guardian role is shown as Appendix B.

2. Policy statement

2.1 This document defines the Caldicott policy for the NHS Business Services Authority (NHSBSA).

2.2 The Caldicott policy applies to all person identifiable information, regardless of whether it is of a medical nature or not, obtained and processed by the NHSBSA and its employees.

2.3 This document:

- sets out the organisation’s policy for the protection of all person identifiable information obtained and processed
- establishes the responsibilities for Caldicott Guardianship
provides reference to the Caldicott principles

3. **Principles**

3.1 Person identifiable information takes many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

3.2 The NHSBSA must safeguard the integrity, confidentiality, and availability of sensitive information.

3.3 No one from the NHSBSA (this includes staff employed by commercial partners and volunteer groups) is allowed to share any person identifiable information unless it has been authorised by the NHSBSA Caldicott Guardian. It is unlikely that this authorisation will be granted unless the access is on a need to know basis and justifiable against the Caldicott principles.

3.4 The Caldicott standard is based around seven principles:

**Principle 1. Justify the purpose(s) for using confidential information**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2. Don’t use personal confidential data unless it is absolutely necessary**

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3. Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4. Access to personal confidential data should be on a strict need-to-know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

4. Scope of this policy

4.1 This policy applies to all person identifiable information processed, stored on computer or relevant filing systems (manual records) and the NHSBSA staff who use the information in connection with their work.

5. Associated legislation

5.1 Apart from the Caldicott standard (including Caldicott2 recommendations) and The Caldicott Guardian Manual 2010, other legislations relevant to the protection and use of person identifiable information must be considered. These include (see appendix A for an explanation of these):

- Data Protection Act 1998
- Human Rights Act 1998
- The Computer Misuse Act 1990
- The Access to Health Records 1990
- Access to Medical Reports Act 1988
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidentiality.

6. Training, policies and procedures

6.1 The NHSBSA takes its responsibilities for the security and protection of all person identifiable information very seriously.
6.2 NHSBSA staff have a responsibility for compliance to the legislation and Caldicott standard. To this end the NHSBSA has:

- confidentiality clauses in employment contracts which each employee signs
- an employee pamphlet
- computer based training programmes (including completing a competency test)
- a specific module that the Caldicott Guardian has to complete on appointment via the HSCIC IG Toolkit, which includes a competency test
- policies, procedures and agreements to ensure any transfer of person identifiable information is compliant.

7. **Advice and guidance**

7.1 The provision of advice and guidance regarding the Caldicott standard and other relevant legislation may be obtained from the Head of Internal Governance.

8. **Validity of this policy**

8.1 This policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

8.2 This policy should be reviewed annually by the Caldicott Guardian.
Appendix A

Data Protection Act 1998 – Data protection principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

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

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

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

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

7. 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.

8. 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.

Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual’s human rights. This will include an individual’s right to privacy (under Article 8) and a service user’s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence’. However, this article also states ‘there shall be no interference by a public authority with the exercise of this right except as is in
accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

Each organisation must act in a way consistent with these requirements. It must take an individual’s rights into account when sharing personal information about them.

**The Computer Misuse Act 1990**

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

**The Access to Health Records 1990**

This Act gives patient’s representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person’s records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

**Access to Medical Reports Act 1988**

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

**Confidentiality: NHS Code of Practice**

The code gives NHS bodies guidance concerning the required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients’ consent to the use of their health records. It replaces previous guidance, HSG (96)18/LASSL (96) 5 – The Protection and Use of Patient Information and is a key component of emerging information governance arrangements for the NHS.
Appendix B

NHS Business Services Authority

Job description

Post: Caldicott Guardian

Band: X

Location: X

Job summary

The appointment of a Caldicott Guardian was one of the recommendations of the Caldicott Report published in December 1997. The role of the guardian is to safeguard and govern uses made of person-identifiable information within the NHS Business Services Authority (NHSBSA), as well as data flows to other NHS and non-NHS organisations.

The Guardian is responsible for the establishment of procedures governing access to, and the use of person-identifiable information and, where appropriate, the transfer of that information to other bodies.

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health.

To provide advice and support to staff working within the NHSBSA on all aspects of Caldicott, sharing and disclosure of person-identifiable patient information and related legislation.

Duties and responsibilities

1. Production of procedures, guidelines and protocols
1.1 To develop and implement procedures to ensure that all routine uses of person-identifiable patient information are identified, agreed as being justified and documented.

1.2 To develop and implement criteria and a process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes.

1.3 To establish Information Sharing Protocols to govern the use and sharing of person-identifiable patient information between organisations both within and outside the NHS.

1.4 To ensure standard procedures and protocols are in place to govern access to person-identifiable patient information.

2. Information for staff

2.1 To ensure standard procedures and protocols are in an understandable format and available to staff

2.2 Raise awareness through training and education to ensure that the standards of good practice and Caldicott principles are understood and adhered to.

2.3 Advise project leads on all aspects of Caldicott, acting as an expert resource for them.

3. Reporting

3.1 To bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.

3.2 To raise concerns about any inappropriate uses made of patient information with the Chief Executive where necessary.

3.3 On an annual basis, to participate in the Information Governance Toolkit Assessment.

3.4 Advise the Chief Executive and the NHSBSA Board on all aspects of processing person-identifiable patient information.

3.5 Should advise the Board/senior management team or the Accounting Officer of any issues relating to confidentiality and data protection assurance so that they can be included within the Statement of Internal Control.

3.6 Should ensure that results of internal audits relating to confidentiality and data protection assurance are appropriately discussed by the Board/senior management team. This will include advising them on confidentiality strategy to implement any necessary improvements.

3.7 Where external audits reveal areas of concern relating to confidentiality and data protection assurance, the Caldicott Guardian should ensure that the Board/senior management team is made aware of the implications and presented with options for improvement.

Working relationships

Accountable to: Chief Executive
Liaises with: The Caldicott Guardian will be expected to liaise and work with business area management and the NHSBSA Board in the course of promoting the Caldicott principles, which will include attendance at various meetings as appropriate.

The Caldicott Guardian is an executive director of the NHS Business Services Authority Board.

The Caldicott Guardian is supported by the Information Governance Manager.
Notes

1. The duties and responsibilities outlined above are to be regarded as broad areas of responsibility and do not necessarily detail all tasks which the post holder may be required to perform.

2. This job description may be subject to change in the light of experience and circumstances and after discussion with the post holder.

3. The post holder will undertake such other duties as may be required commensurate with grade and experience.

4. The post holder will be expected to act with full regard to the requirements of the Authority's policies and procedures, including those relating to health and safety.