NHS Counter Fraud Authority

Caldicott policy

September 2018

Version 2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
1.0	Trevor Duplessis	22/01/18	Review May 2018
2.0	Trevor Duplessis	September 2018	Update

Table of contents

1. Introduction

1.1 This document describes the NHS Counter Fraud Authority's (NHSCFA) policy on Data Protection and Caldicott requirements and its employees' responsibilities, for the safeguarding of confidential information whether held manually (in a structured filing system) or electronically.

1.2 NHSCFA holds and manages personal and confidential information relating to individuals, the public and employees of the organisation.

1.3 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use personal and sensitive data for legitimate business purposes. They work to provide individuals with certain rights, whilst imposing certain responsibilities on those who record and use personal information.

1.4 In December 1997 the Caldicott Report identified weaknesses in the way NHS organisations handled confidential patient identifiable information. It introduced and defined the Caldicott principles and created the role of the Caldicott Guardian.

1.5 One of the recommendations stated that all NHS organisations appoint a Caldicott Guardian to ensure patient identifiable information is kept secure. The recommendation being that Caldicott Guardians should be senior members of staff, preferably at board level.

1.6 Sue Frith, the NHSCFA's Interim Chief Executive, has been appointed as the organisation's Caldicott Guardian. An outline of the job responsibilities for the Caldicott Guardian's role is shown at Appendix A.

2. Policy statement

2.1 This document defines the Caldicott policy for the NHSCFA and sets out the framework to ensure the organisation complies with the law.

2.2 The Caldicott policy applies to all person identifiable information, regardless of whether it was originally obtained and processed by the NHSCFA and its employees or acquired through a third party.

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 NHSCFA must safeguard the integrity, confidentiality, and availability of sensitive information it holds.

3.3 No one from the NHSCFA is allowed to share any person identifiable information unless it has been approved by the NHSCFA Caldicott Guardian (via the Information Governance Team). 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 and stored on computer or relevant filing systems (manual records) and the NHSCFA staff who use the information in connection with their work.

4.2 It also provides an overview of the responsibilities of the named Caldicott Guardian(s) as well as providing all employees and partner organisations with an understanding of their responsibilities in ensuring the Caldicott Guardian's views and sign-off are appropriately sought as and when required.

4.3 All employees handling personal confidential data on behalf of the NHSCFA have a personal responsibility, where appropriate to engage the Caldicott Guardian and/or the Information Governance & Risk Management Lead.

5. Associated legislation

5.1 In addition to the Caldicott standard (including the Caldicott2 recommendations) and the Caldicott Guardian Manual 2017, there are other legislative and common

law provisions relevant to the use and protection of person identifiable information that must be considered. These include but are not limited to:

- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018
- 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.

See appendix A for brief explanation of each.

6. Training, policies and procedures

6.1 NHSCFA staff have a responsibility to comply with legislation and the Caldicott standard. To this end the NHSCFA has:

- confidentiality clauses in employment contracts which the employee is required to sign
- a new-starter induction pack
- computer based training programmes (including completing a competency test)
- annual refresher training
- policies, procedures and agreements to ensure any processing and/or 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 Information Governance Lead.

8. Validity of this policy

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

8.2 This policy will be subject to regular planned review, at least annually by the Caldicott Guardian or sooner if required via the Information Governance Lead or the IT Security Forum, where there are changes in legislation or recommended improvements to best practice.

Appendix A - Caldicott Guardian job description

NHS Counter Fraud Authority

Job responsibilities

Post: Caldicott Guardian

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 Counter Fraud Authority (NHSCFA), 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 Information Management and Training (IM&T) security disseminated by the Department of Health and Social Care.

To provide advice and support to staff working within the NHSCFA 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 person-identifiable information with the Information Governance & Risk Management Lead where appropriate.

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

3.4 Advise the NHSCFA Board on all aspects of processing person-identifiable information.

3.5 Should advise the Board/Senior Management Team or the Information Governance & Risk Management Lead 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

Liaises with:

The Caldicott Guardian will be expected to liaise and work with the NHSCFA Board, the Senior Management Team and the Information Governance & Risk Management Lead in the course of promoting the Caldicott principles, which will include attending various meetings as appropriate.

The Caldicott Guardian is the Chief Executive of the NHSCFA.

The Caldicott Guardian is supported by the Information Governance Manager and the Head of Operations.

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. The 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