

# Caldicott policy

October 2019

FCG-IG-CP-017 Version 3.0



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

## Version control

Version	Name	Date	Comment
V.1.0	Finance & Corporate Governance	January 2018	Review August 2018
V.2.0	Finance & Corporate Governance	August 2018	Annual Review August 2019
V.3.0	Finance & Corporate Governance	October 2019	Annual Review October 2020

## Table of contents

<b>1. Introduction.....</b>	<b>4</b>
<b>2. Policy statement .....</b>	<b>4</b>
<b>3. Principles .....</b>	<b>5</b>
<b>4. Scope of this policy .....</b>	<b>6</b>
<b>5. Associated legislation .....</b>	<b>6</b>
<b>6. Training, policies and procedures.....</b>	<b>7</b>
<b>7. Advice and guidance.....</b>	<b>7</b>
<b>8. Validity of this policy .....</b>	<b>8</b>
<b>Appendix A - Caldicott Guardian job description .....</b>	<b>9</b>
<b>Appendix B - Summary of legislative and common law provisions .....</b>	<b>12</b>

## 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 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 either the Caldicott Guardian 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 B 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.

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 NHSBSA 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

## **Appendix B - Summary of relevant legislation and common law provisions**

### **The General Data Protection Regulation (GDPR) and Data Protection Act 2018**

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

The primary aims of GDPR are to give control to individuals over their personal data and to simplify the regulatory environment for international organisations by unifying the regulation within the EU.

The Data Protection Act 2018 sets out and updates the framework for data protection law in the United Kingdom (UK). It sits alongside the EU's GDPR and tailors how it applies in the UK. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence and sets out the Information Commissioner's functions and powers.

### **Human Rights Act 1998**

This Act binds public authorities including Health Authorities, Trusts and Primary Care Groups 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. NHSCFA issues each employee with an individual user id and password which will only be known to the individual and must not be

divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

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

## **Access to Health Records Act 1990**

Under this Act all patients have a right to request access to all of their healthcare records. Persons wishing to access the records of a deceased individual may also do so under the Act.

## **Access to Medical Reports Act 1998**

The Act gives patients the right to see reports written about them by a doctor for employment or insurance purposes within whom they have a normal doctor-patient relationship.

Access to a report can be withheld if the doctor thinks it is likely to cause serious harm to the physical or mental health of the individual or others or indicate the intentions of the practitioner in respect of the individual, or to reveal the identity of another person who has supplied information.

## **Confidentiality: NHS Code of Practice**

This 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 personal data.

## **Common law duty of confidentiality**

Common law is also referred to as 'judge-made' or case law; it is applied by reference to previous case judgements and so is also said to be based on precedent.

The general position is, where information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information providers consent.

The duty of confidentiality is not an absolute right. There are circumstances where making the disclosure of confidential information is lawful:

- where the individual to whom the information relates has consented
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest

## OFFICIAL

- where there is a legal duty to do so (such a court order)