Bath & North East Somerset Council

B&NES Council People and Communities Department

Caldicott Guardian Function Plan 2015-17

Author:	**Lesley Hutchinson**
Version:	**1**
Approving Group:	**People and Communities SLT**
Approved:	**1.02.2016**
Review Date Due:	**1.04.2017**

Contents **Page**

Appendix

1. Introduction

1.1 The Caldicott Report 1997

In 1997 the Department of Health's Chief Medical Officer of England commission the Caldicott Committee (Chaired by Dame Fiona Caldicott) to review the transfer of patient-identifiable information from NHS organisations to other NHS and non-NHS organisations. The review was commissioned because of the increasing concern about the ways in which patient information was being used and the Department of Health sought assurance that confidentiality was not being undermined. The Committee in its report *The Caldicott Report* 1997 (Report on the Review of Patient-Identifiable Information) put forward 16 recommendations and suggested six principles which were to be applied to the flows of information.

http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

The Caldicott Report primarily focussed on the way NHS organisations shared information, however it makes reference to the sharing of information with Social Services (2.1.5 p5) and refers to the need to provide 'seamless care' offering a framework for the sharing of personal information with non-NHS bodies including Social Services.

The aim of the Report was to ensure that patient identifiable information was shared only for justifiable purposes and that only the minimum necessary information was shared in each case. It recommended that NHS organisations appoint a 'Guardian' to oversee the arrangements for sharing patient identifiable information and for these arrangements to be measured against a set of principles – commonly known as the Caldicott Principles.

1.2 The Data Protection Act 1998

In 1998 the Data Protection Act was passed and came into force in early 1999. It updates the previous 1994 Act and controls how personal information is used by organisations, business and the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- *used fairly and lawfully*
- *used for limited, specifically stated purposes*
- *used in a way that is adequate, relevant and not excessive accurate*
- *kept for no longer than is absolutely necessary*
- *handled according to people's data protection rights*
- *kept safe and secure*
- *not transferred outside the European Economic Area without adequate protection*

There is stronger legal protection for more sensitive information, such as:

- *ethnic background*
- *political opinions*
- *religious beliefs*
- *health*
- *sexual health*
- *criminal records* (Gov.uk website)

1.3 Caldicott Guardians and Local Authorities'

In 2002 Caldicott Guardians became a requirement for social care and was mandated by the Local Authority Circular *(LAC 2002/2 – Implementing the Caldicott Standard into Social Care appointment of Caldicott Guardians).*

http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4012746.pdf

'The Caldicott standard is being extended into Councils with Social Services Responsibilities in order to provide a good foundation for joint working between health and social services, and to help support the fulfilment of the many joint strategies across children's and adult services.

The Data Protection Act 1998 is the key legislation covering all aspects of information processing, including security and confidentiality of personally identifiable information. The Caldicott requirements provide a framework to operationalise the Data Protection Act and underpin appropriate information sharing. (p2)

1.4 The Caldicott2 Review

In 2012 Dame Fiona Caldicott carried out an independent review of information sharing. The review sought to ensure there is an appropriate balance between the protection of *patient* (service user) information and the use and sharing of information to improve *patient* (service user) care. The review report was published in 2013 and contained 26 recommendations**.**

The Report - *Information: To Share or Not to Share? The Information Governance Review* (DH 2013) was overseen by an Independent Information Governance Oversight Panel (set up at the request of the Secretary of State for Health) and is commonly known as Caldicott2 Review. The review made slight amendments to the original 1997 Report and added an additional one making it seven. 26 recommendations were made in all and the Government accepted them.

https://www.gov.uk/government/publications/the-information-governance-review

1.5 The Caldicott Principles

There are seven Principles that must be adhered to:

1. Justify the purpose(s)
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.

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).

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.

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.

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.

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.

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. (p20, 2013)

1.6 UK Council of Caldicott Guardians

There is a UK Council of Caldicott Guardians which meets four times a year. The Councils Constitution can be found at the web link below though has not been revised since 2008 (according to the website).

http://systems.hscic.gov.uk/infogov/caldicott/membership/councilsconstitution.pdf

The Council has a 5 year strategy 2011-2016.

http://systems.hscic.gov.uk/infogov/links/strategy2011.pdf

The three primary objectives of the strategy are:
1. Providing leadership on Caldicott and confidentiality matters
2. Develop the skills and wisdom of all Caldicott Guardians
3. Innovations and practice developments

1.7 Other Legislation Relevant and Influencing the Caldicott Guardian

In addition to the Caldicott Principles and the Data Protection Act 1998 'Guardians' must pay attention to and work within the following Acts and requirements:

- The Human Rights Act 1998
- The Freedom of Information Act 2000
- The inception of NHS Information Governance 2003
- Information Governance Toolkit 2003
- The Cayton review of NHS Information 2006
- Heath and Social Care Information Centre requirements

2. Caldicott Responsibilities

2.1 Role of the Caldicott Guardian

The role of the Caldicott Guardian is set out in the Caldicott Guardian Manual 2010 (DH – written by the UK Council of Caldicott Guardians) and is part of the broader Information Governance arrangement the Council has in place which the Information Governance Service is accountable for.

http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf

The HSCIC states the Guardian should be:

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. (UK Council of Caldicott Guardians 5 Year Strategy p6 also one of the recommendations in the 1997 Report)

They should:

Act… as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

and have

...a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

This role is particularly important in relation to the implementation of the national systems and the development of Electronic Social Care Records and Common Assessment Frameworks. (HSCIC website)

The Guardian is also responsible for:

- Ensuring the Caldicott Principles are adhered to
- Ensuring procedures that affect access to persons-identifiable information are adhered to (including subject access requests)
- Ensuring the person's right to confidentiality is adhered to
- Ensuring information sharing arrangements are adhered to
- Ensuring breaches are reported and action plans adhered to
- Contributing to the annual assessment
- Providing routine reports to senior management on confidentiality and data protection issues

NHS and Social Care Guardians are required to be registered on the publicly available National Register of Caldicott Guardians and in B&NES Council the role is fulfilled by the Head of Safeguarding and Quality Assurance in the Directorate for People and Communities. Lesley Hutchinson is the current postholder and is registered for B&NES Council with the Health and Social Care Information Centre (HSCIC).

2.2 Impact for People and Communities Staff

People and Communities staff must ensure they adhere to the seven Caldicott Principles (set out in 1.5). By adhering to these every employee is responsible for information security and confidentiality ensuring that:

- Any information obtained, either directly or indirectly from or about a service user is not disclosed to any person, organisation or body who does not need to know or who does not have an authorised right to access that information.
- Every use or transfer of personal information, including e-mail, is clearly justified. Personal information should not be used unless it is absolutely necessary.
- Consent is sought wherever possible for the recording, retention and sharing of personal information.

- Appropriate information is shared with other professionals if it is in the best interests of the service user or is necessary to safeguard another professional.
- Wherever appropriate, personal information is anonymised such as for statistical reporting.
- Reasonable steps are taken to ensure that all information recorded is accurate and up-to-date and that information is only changed or modified by someone authorised to do so. (If a service user advises that their information is incorrect that a correction is made immediately or a note added to the file if correction is not possible or inappropriate).
- Records are maintained for the required period and no longer.
- Security passwords are not be shared with any other person.
- Service user records are not kept for longer than necessary.
- Service user records are not accessed unless there is a business reason for the access.

2.3 Procedure of a Data Breach Occurs

Four steps must be followed if a data breach occurs these are set out in the Procedure for Handling a Data Breach (see Appendix 1):

Step 1: Identification and notification – the Security Incident and Data Breach Management Response Plan Template is attached as Appendix 2.
Step 2: Investigation
Step 3: Reporting
Step 4: Monitoring

People and Communities will monitor data breaches on a quarterly basis.

2.4 Support from the Caldicott Guardian, Complaints and Data Protection Team and Information Governance Team

Requests for information may come from a variety of sources. The Complaints and Data Protection Team will oversee Subject Access Requests with support from Children Social Care team managers. Where other requests regarding the release of personal identifiable information are received People and Communities staff can seek advice from either the Caldicott Guardian or the Complaints and Data Protection team who will in turn liaise with the Information Governance Team regarding approval of the release. Approval must be sought and confirmed.

All requests requiring approval will be logged and reported.

The Information Governance Team, are responsible for providing support and advice on all aspects of information governance including information sharing issues. Staff must be aware of the following:

Managing the councils information security arrangements eg, complaince with Government Connect (GCSx)	http://intranet/government-connect
GlobalSCAPE	http://intranet/globalscape
Outlook Web Access Policy	http://intranet/outlook-web-access-policy
Emails and Internet Guidelines	http://intranet/email-and-internet-access-guidelines
G-drive guidelines	http://intranet/g-drive-guidance
Advising on record retention / record management (follow the link through social care)	http://intranet/ims-record-retention
Confidential Waste and Council Policy	http://intranet/ims-confidential-waste
Clear workspace arrangements etc	http://intranet/clear-workspace-guidelines
Securely Transferring Information Guidelines	http://intranet/securely-transferring-information-guidelines

3. Strategic Action Plan

Aim	Action	Implementation by:
1. Ensure effective communication regarding Calidcott Principles and data protection across People and Communities	Review website information on Caldicott Principles	February 2016
	Share Caldicott Function Plan across the Directorate	February 2016
	Provide an update about the Function Plan at staff briefings each time the plans is reviewed	Next round of staff briefings
	Quarterly meetings with Caldicott Guardian, Complaints Procedure and Data Protection Team Manager and Information Governance Team to be established	January 2016 April 2016 July 2016 October 2016
2. Review Directorate workforces understanding and aware of their roles	Include Caldicott Principles as part of new staff induction programmes	Beginning of March 2016

and responsibilities	Undertake departmental survey to gather baseline position on ensure staffs understanding of Caldicott and information sharing requirements	June 2016
	Caldicott Principles to be discussed at annually by each team – Directors to monitor this and report to Caldicott Guardian each March	Commence from March 2016
3. Monitor compliance with procedure for handling data protection breaches	Annual report to be provided by Information Governance Team and Caldicott Guardian (to include quantitative and thematic information)	May 2016 and each May for the life of the Plan
4. Develop learning opportunities for the Caldicott Guardian and Complaints Procedure and Data Protection Team Manager	Access to appropriate training to assist in their role – through either online or external training as appropriate	As and when needed when new developments are implemented
	Access support through regional and national forums	As and when needed
5. Review the information available on information sharing for service users and families, including leaflets and information on the website	Review documentation and accessibility	March 2016
6. Review training opportunities for staff within People and Communities	Work with Information Governance Team and training staff to agree the offer / minimum requirement and expectation for staff appropriate to their position	September 2016
7. Ensure arrangements with Sirona Care and Health and AWP in relation to non	Review reporting requirements for Sirona and AWP in relation to non delegated responsibilities	March 2016

delegated responsibilities	If required set up new reporting arrangements from April 2016	
8. Scope support that maybe required with other Directorates in relation to Caldicott functions	Work with the Information Governance Team to identify the support required across the other Council Directorates	April 2016

Appendix 1

People and Communities Department

Procedure for Handling a Data Breach

What is a Data Breach?

A data breach is considered to be any loss of, or unauthorised use of data, normally personal or confidential data. Data breaches include the loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

Why Have a Data Breach Policy?

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

Every care should be taken to protect information and to avoid a data breach, however, in the unlikely event of a breach it is vital that appropriate action is taken to minimise any associated risk as soon as possible. There should be a standardised process in place for dealing with the breach to ensure the breach is reported to the Information Governance Team (IGT) for investigation and reporting, if required. This procedure sets out what that process is for People and Communities staff.

Managing a Data Breach

Data breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Serious breaches of the Data Protection Act can result in fines of up to £500,000 per breach and significant reputational damage, and may require substantial time and resources to rectify the breach. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

Step1: Identification and notification - as soon as you become aware of a data breach you should:

- Take action to ensure that there is no further loss of data e.g. inform IT so that a tablet or laptop can be locked;
- Inform your manager to agree who else should be informed at this stage;
- Complete the Security Incident and Data Breach Management Response Plan Template found here and send to IGT;
- Send a copy of the form addressed to the Complaints Procedure and Data Protection Manager via james_bosanquet@bathnes.gov.uk (the Data Protection and Complaints Officer).

Step 2: Investigation – IGT will investigate the incident in conjunction with the service. This could involve the service in reviewing existing systems and procedures, interviewing staff and staff from other agencies.

Step 3: Reporting – when the investigation is complete the IGT will advise the manager what further action is required by the service to respond to the data breach and reduce the risk of a similar event occurring in the future. This could include:

- The LA reporting the incident to the Information Commissioner's Office (ICO). This could result in further investigation and a possible fine by the ICO;
- The LA reporting the incident through the HSCIC IG incident reporting tool, which is published quarterly
- Informing the person/s whose data has been lost or inappropriately shared. Standard letters for writing to service users are available from the Data Protection and Complaints Officer;
- A change to procedures and working practices;
- Advise sought from HR on appropriate procedures to be used to address the issue with an individual member of staff (e.g. disciplinary or capability procedures).

Step 4: Monitoring – this stage is important to prevent further occurrence of the same type of breach or similar.

- The outcome of the investigation will be sent to the person who reported the breach. A copy should be sent to the Data Protection and Complaints Officer;
- The Complaints Procedure and Data Protection Manager will complete a quarterly report for the Head of Safeguarding and Quality Assurance on the number, severity and outcome of all data breaches recorded during the quarter. This report will be used to ensure the risk of a further data breach is minimised.

Author: Sarah Watts, Complaints Procedure and Data Protection Manager
Written: January 2016
Approved: 1.02.2016
Approved by: Senior Leadership Team, People and Communities
For review: January 2018

Appendix 2 – Security Incident and Data Breach Management Response Plan Template

Bath & North East Somerset Council

Security Incident & Data Breach Management

Response Plan Template

Please complete Section 1 of this form and return to the Information Governance Manager amy_ogborne@bathnes.gov.uk when any event occurs that threatens the confidentiality, integrity or the availability of information. This is a requirement of the Data Protection Act 1998, Caldicott recommendations and ISO/IEC 27002:2005 Code of Practice for Information Security Management. This Response Plan Template describes the actions that users are to follow after an incident.

Section 2 will be completed by the Investigating Officer who will keep you updated on progress.

Confidentiality

Distribution of this document is limited. Access should only be granted to those with a business related need-to-know. If you have any questions pertaining to the distribution of this document, please contact the Council's Information Governance Manager amy_ogborne@bathnes.gov.uk telephone 01225 396872 or Information_Governance@bathnes.gov.uk

SECTION 1

Reporting Officer Contact Details

Name (of person who discovered the incident):
Title:
Organisation/Service:
Location:
Logon:

e-mail Address: **Telephone**:

Incident Details

Date/|Time Occurred (if known): **Date/|Time of Discovery**: **Date/Time Reported**:	**Location of Incident**: **Incident Type**: Please see attached listing

Executive Summary of the Incident: At a high level, suitable for senior management. It is to include: Basic description of incident: Root cause and details of which information was affected. Contacts details of all people involved in the incident: Systems, services and organisations impacted, degraded or interrupted by the incident: Duration of the incident (start to finish):

Brief Description of Any Action Taken (at time of discovery):

SECTION 2

Information Governance Team

Incident Reference: **Suggested Incident Classification**:	**Date Central Record Updated**:
Date Notified:	**Date Caldicott Guardian informed**:

Details of the Incident: Specifically what caused the incident (who, what, where, when and how) – include as much detail as possible.

Details of the Incident / Fix Actions: When and by whom Provide evidential details
Brief Description of Action Taken by Information Governance Team / Caldicott Guardian:

Remediation- Conclusion and Lessons Learned: To include: Specifically what was the basic cause of the incident: What could have prevented this: Impact: Business criticality: Estimated cost: What prevents the incident from re-occurring?: What additional actions or research need to happen?:
Appendices:
Date of Intended Follow-up:

Brief Description of Follow-up Action(s) Required:

Name: ……

Title: ……

Date: ……

Appendix A

Bath & North East Somerset Council

Security Incident Management

Definition and Classification Matrix

Definition

The Council has defined an information security incident as an adverse event that has caused, or has the potential to cause, damage to the Council's, reputation and or personnel.

In summary this may involve any or all of the following:

- unauthorised computer access
- loss of information confidentiality
- loss of information availability
- compromise of information integrity
- misuse use of service, systems or information, or
- physical or logical damage to systems

More detailed examples of an incident include:

Unauthorised Access

- to a network, system, information, IT assets and secure buildings
- compromised or sharing of user credentials
- inappropriate access following changes in job roles and responsibilities
- system account compromise
- establishment of an authorised account
- disclosure of information to any unauthorised person
- unusual network connections to a computer
- breaches of physical security arrangements

Systems

- use of Council equipment to store personal information
- abuse of system access to personal information not related to a user's job, for personal or other reasons, including curiosity
- Council software subjected to piracy, inadvertent or malicious deletion or amendment
- information lost or stolen, subject to amendment or falsification
- system or computer loss or performance degradation
- system overload
- malfunctions or uncontrolled system changes

Hardcopy and Removable Media

- hardcopy paper documentation left in an unsecured location, including printer rooms
- unprotected CD/DVDs, diskettes and microfiche retained insecurely
- unprotected portable equipment used to exchange information, including handheld, mobile phones and cameras

Hardware

- misappropriated, lost or damaged
- malfunction

Loss due to crime or carelessness

- equipment, including removable media such as memory sticks and CDs
- physical break-in

Malicious Code & Social Engineering

- virus, worm or trojan infection used to gain privileges, capture passwords and/or modify audit logs to hide unauthorised activity
- spamming and phishing
- presence of unexpected programs/files
- unexpected application response
- network attacks (denial of service, scanning, sniffing)

Miscellaneous

- non-compliance with policies, protocols or guidelines
- hoaxes – the spreading of false information about incidents and vulnerabilities
- human error

If there is any doubt as to whether an event constitutes an incident (breach or weakness), or whether it is appropriate to report it, further advice and support should be sought immediately from the Information Governance Manager amy_ogborne@bathnes.gov.uk or Information_Governance@bathnes.gov.uk