The Clatterbridge Cancer Centre
NHS Foundation Trust

Report Cover Sheet

Report to:	Board of Directors	
Date of the Meeting:	25 September 2019	
Agenda Item:	P1/184/19	
Title:	Caldicott Guardian Annual Report	
Report prepared by:	Andrew Ivers, Information Governance Manager (Data Protection Officer)	
Executive Lead:	Sheena Khanduri, Medical Director and Caldicott Guardian	
Status of the Report:	Public	Private
	X	

Paper previously considered by:	Information Governance Board Meeting
Date & Decision:	16/09/2019

Purpose of the Paper/Key Points for Discussion:	The Caldicott Guardian has a key role in ensuring that the Trust achieves the highest practical standards for handling patient information. This includes representing and championing confidentiality requirements and issues at Board Level, and wherever appropriate within the Trust's overall governance framework. The key Caldicott Guardian responsibilities as defined in the Department of Health Caldicott Guardian Manual (2017) are: **1.** Strategy and Governance **2.** Confidentiality and Data Protection expertise **3.** Internal Information Processing Information Sharing It is a requirement within the NHS Standard Contract. This report is required annually as a summary of the work undertaken in this role

Action Required:	Discuss	
	Approve	
	For Information/Noting	X

Next steps required	

The paper links to the following strategic priorities (please tick)

Deliver **outstanding care locally**	x	Collaborative system **leadership** to **deliver better** patient **care**	
Retain and **develop outstanding staff**		Be **enterprising**	
Invest in **research & innovation** to deliver **excellent** patient **care** in the future		Maintain **excellent** quality, operational and financial **performance**	x

The paper relates to the following Board Assurance Framework (BAF) Risks

BAF Risk	**Please Tick**
1. If we do not optimise quality outcomes we will not be able to provide outstanding care	
2. If we do not prioritise the costs of the delivering the Transforming Cancer Care Programme we will not be able to maintain our long-term financial strength and make appropriate strategic investments.	
3. If we do not have the right infrastructure (estate, communication & engagement, information and technology) we will be unable to deliver care close to home.	x
4. If we do not have the right innovative workforce solutions including education and development, we will not have the right skills, in the right place, at the right time to deliver the outstanding care.	
5. If we do not have an organisational culture that promotes positive staff engagement and excellent health and well-being we will not be able to retain and attract the right workforce.	
6. If we fail to implement and optimise digital technology we will not deliver optimal patient outcomes and operational effectiveness.	
7. If we fail to position the organisation as a credible research partner we will limit patient access to clinical trials and affect our reputation as a specialist centre delivering excellent patient care in the future.	
8. If we do not retain system-side leadership, for example, SRO for Cancer Alliance and influence the National Cancer Policy, we will not have the right influence on the strategic direction to deliver outstanding cancer services for the population of Cheshire & Merseyside.	
9. If we do not support and invest in entrepreneurial ideas and adapt to changes in national priorities and market conditions we will stifle innovative cancer services for the future.	
10. If we do not continually support, lead and prioritise improved quality, operational and financial performance, we will not provide safe, efficient and effective cancer services.	x

Equality & Diversity Impact Assessment		
Are there concerns that the policy/service could have an adverse impact on:	YES	NO
Age		x
Disability		x
Gender		x
Race		x
Sexual Orientation		x
Gender Reassignment		x
Religion/Belief		x
Pregnancy and Maternity		x

If YES to one or more of the above please add further detail and identify if a full impact assessment is required.

The Clatterbridge Cancer Centre
NHS Foundation Trust

Caldicott Guardian Report
January 2018 to March 2019

Executive Summary:

The Caldicott Guardian has a key role in ensuring that the Trust achieves the highest practical standards for handling patient information. This includes representing and championing confidentiality requirements and issues at Board Level, and wherever appropriate within the Trust's overall governance framework.

The key Caldicott Guardian responsibilities as defined in the Department of Health Caldicott Guardian Manual (2017) are:

4. Strategy and Governance
5. Confidentiality and Data Protection expertise
6. Internal Information Processing
7. Information Sharing

The appointment of a Caldicott Guardian was mandated for the NHS by a Health Service Circular: HSC 1999/012 and was subsequently introduced into Social Care in 2002, mandated by Local Authority Circular: LAC 2002/2. Since the mandates, all NHS organisations and local authorities providing social services must have a Caldicott Guardian, who must be registered on the publicly available Caldicott Guardian Register, available on the NHS Digital website at: https://digital.nhs.uk/organisation-data-service/our-services.

It is also a requirement within the NHS Standard Contract; *section GC21 - Patient Confidentiality, Data Protection, Freedom of Information and Transparency* for "providers" to……

> "*…… nominate a **Caldicott Guardian** and Senior Information Risk Owner, each of whom must be a member of the Provider's Governing Body"*
>
> *".……ensure that the Co-ordinating Commissioner is kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, **Caldicott Guardian** and the Senior Information Risk Owner"*
>
> *".……ensure that NHS England and NHS Digital are kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, **Caldicott Guardian** and the Senior Information Risk Owner via the NHS Data Security and Protection Toolkit."*

This report is required annually as a summary of the work undertaken in this role.

1. Introduction

The Caldicott Guardian (named after the Chair of a Committee which defined the required patient confidentiality standards and processes in the NHS) has a key role in ensuring that the Trust achieves the highest practical standards for handling patient information. This includes representing and championing confidentiality requirements and issues at Board Level, and wherever appropriate within the Trust's overall governance framework.

The key Caldicott Guardian responsibilities as defined in the Department of Health Caldicott Guardian Manual (2017) are:

> **Strategy & Governance:** the Caldicott Guardian should champion confidentiality issues at Board/senior management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.
>
> **Confidentiality & Data Protection expertise**: the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.
>
> **Internal Information Processing**: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Data Security & Protection Toolkit.
>
> **Information Sharing**: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related new IT systems, disclosure to research interests and disclosure to the police.

2. The Caldicott Guardian role at The Clatterbridge Cancer Centre

Up until 28th February 2018 the role of Caldicott Guardian at the Trust was part of the Executive Director of Nursing & Quality's portfolio. Up until that date this role was occupied by Helen Porter. From the 1st April 2018, the role was transferred to the portfolio of the Trust's Medical Director, currently occupied by Dr. Sheena Khanduri.

3. Report on Compliance

The Caldicott Function is an integral part of the Trust's Information Governance Fraemwork. The Caldicott Guardian works closely with the Information Governance Manager (Data Protection Officer)

As part of the Information Governance work plan, an annual Caldicott Function Plan is a documented which sets out the approach the Trust will take for the forthcoming year ahead in order to discharge its Caldicott responsibilities. The Caldicott Function Plan for 2018-2019 is detailed in *Appendix A*

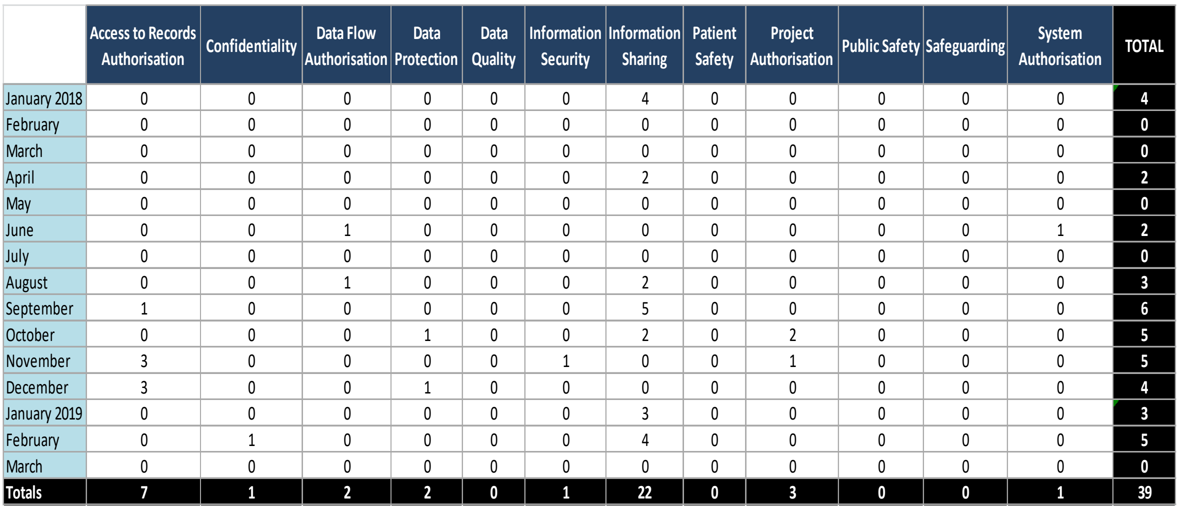
The Caldicott Guardian attends the Information Governance Board.

a. Caldicott Log

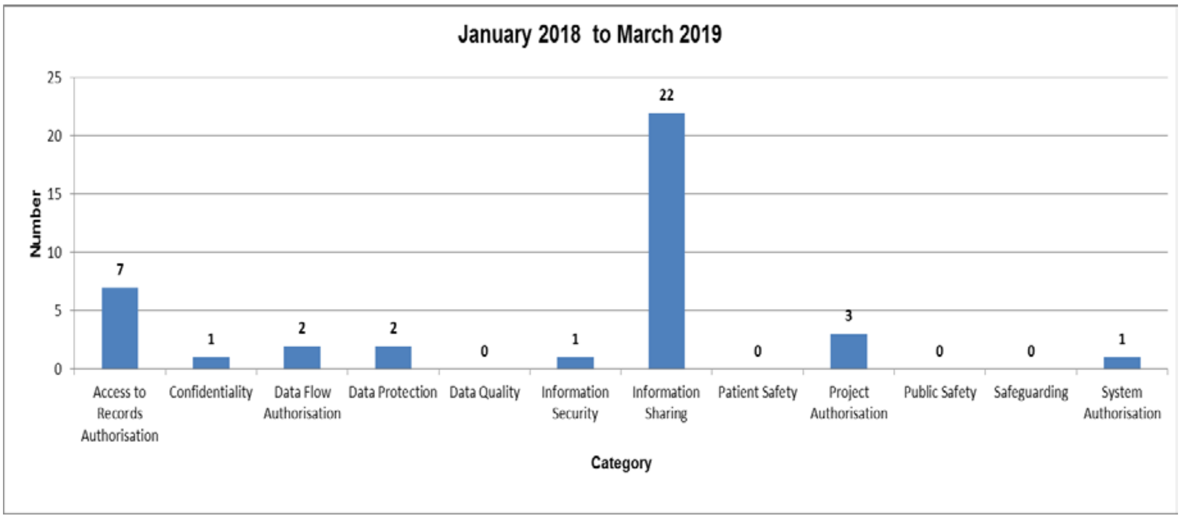
All interventions requiring Caldicott input are recorded in a Caldicott Log. The Caldicott Log is included on the Information Governance Board Meeting agendas and reviewed as standing agenda item.

In total, between January 2018 and March 2019, **39** Caldicott interventions were logged.

Caldicott Activity by Category

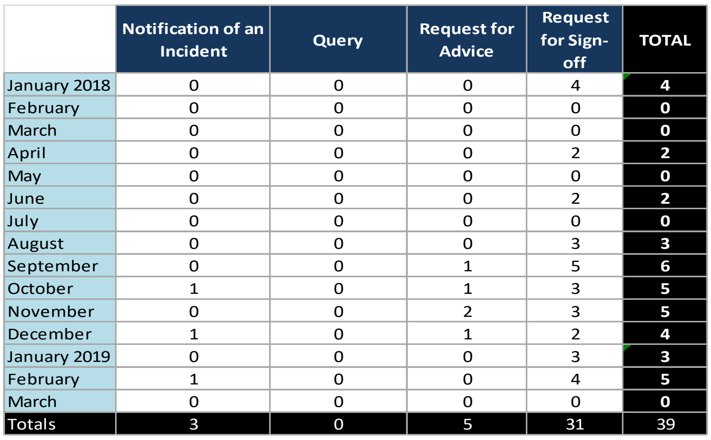


	Access to Records Authorisation	Confidentiality	Data Flow Authorisation	Data Protection	Data Quality	Information Security	Information Sharing	Patient Safety	Project Authorisation	Public Safety	Safeguarding	System Authorisation	TOTAL
January 2018	0	0	0	0	0	0	4	0	0	0	0	0	4
February	0	0	0	0	0	0	0	0	0	0	0	0	0
March	0	0	0	0	0	0	0	0	0	0	0	0	0
April	0	0	0	0	0	0	2	0	0	0	0	0	2
May	0	0	0	0	0	0	0	0	0	0	0	0	0
June	0	0	1	0	0	0	0	0	0	0	0	1	2
July	0	0	0	0	0	0	0	0	0	0	0	0	0
August	0	0	1	0	0	0	2	0	0	0	0	0	3
September	1	0	0	0	0	0	5	0	0	0	0	0	6
October	0	0	0	1	0	0	2	0	2	0	0	0	5
November	3	0	0	0	0	1	0	0	1	0	0	0	5
December	3	0	0	1	0	0	0	0	0	0	0	0	4
January 2019	0	0	0	0	0	0	3	0	0	0	0	0	3
February	0	1	0	0	0	0	4	0	0	0	0	0	5
March	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals	7	1	2	2	0	1	22	0	3	0	0	1	39

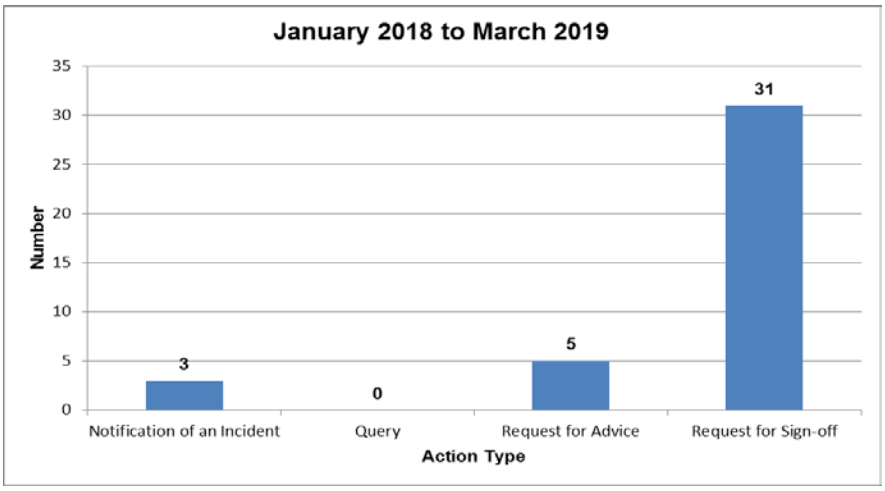


The majority of the interventions logged related to **Information Sharing** (**22**), in particular Information Sharing Agreements, followed by **Access to Record Authorisations** (**7**), which included complex Subject Access Requests, Access to Health Record Act Requests and disclosures to law enforcement agencies.

Caldicott Activity by Action Type



	Notification of an Incident	Query	Request for Advice	Request for Sign-off	TOTAL
January 2018	0	0	0	4	**4**
February	0	0	0	0	**0**
March	0	0	0	0	**0**
April	0	0	0	2	**2**
May	0	0	0	0	**0**
June	0	0	0	2	**2**
July	0	0	0	0	**0**
August	0	0	0	3	**3**
September	0	0	1	5	**6**
October	1	0	1	3	**5**
November	0	0	2	3	**5**
December	1	0	1	2	**4**
January 2019	0	0	0	3	**3**
February	1	0	0	4	**5**
March	0	0	0	0	**0**
Totals	3	0	5	31	39



The majority of the actions performed as a result of an intervention being logged were **Requests for Sign-off** (**31**), in particular Information Sharing Agreements (**22**), Project Authorisations **(3)** and Access to Record Authorisations (**3**)

b. Information Sharing Agreements

Between January 2018 and March 2019 Information Sharing Agreements were kept under review and updated as necessary, and reported through the Information Governance Board. As at the end of March 2019, the Trust has **42** active Information Sharing Agreements, which is an increase of **10** from the previous Caldioctt Guardian Report covering the calendar year 2017. As part of the General Data Protection Regulations implementation work that took place during the reporting period, an abridged version of the Trust's Information Sharing Agreement register was published on the Trust's public facing internet website - https://www.clatterbridgecc.nhs.uk/patients/your-rights/confidentiality-data-protection/information-sharing-agreements. This formed part of a wider update to the Trust's Privacy Notice - https://www.clatterbridgecc.nhs.uk/patients/your-rights/confidentiality-data-protection

c. Information Governance Related Incidents

All reported confidentiality incidents are subject to timely investigation and review of mitigating action. All SUIs are reported directly to the Caldicott Guardian. All incidents are reviewed at the Information Governance Board.

In total, during the reporting period, there were **171** reported Information Governance related/tagged incidents, summarised by Datix Incident Category Tier 3 below:

Incident Type Tier Three	Number of Incidents
Incorrect patient	50
Unintentional breach	**40
Ambiguous/incorrect/incomplete	17
Other	8
Temporarily unavailable/delay in accessing	8
Other documentation incident	6
Confidentiality breach	5
Non-compliance with fair processing requirement	4
Other communication incident	4
Unauthorised disclosure of personal data without consent	4
Omission of important facts	3
Other administration incident	3
Inadequate controls regarding employee access to data	2
Unauthorised access to personal data without consent	2
Abuse/misuse of user privileges	1
Administrative/management policies	1
Data/information	1
Hardware	1
Incorrect consultation/referral	1
Incorrect data	1
Incorrect/insufficient handover	1
Intentional breach	1
No access	1
Paperwork	1
Patient data/information	1

Incident Type Tier Three	Number of Incidents
Permanently unavailable	1
Records inaccurate/not up to date	1
Referral insufficient/incorrect/incomplete	1
Transfer between units/care settings insufficient/incorrect/incomplete	1

*** NB 32 of the 40 incidents are not attributable to the Trust as the breaches occurred at other organisations*

There has been one Serious Incident during the period, which was categorised as level 2 in the Information Governance Incident reporting Tool and, as such, required formal external notification to the Information Commissioner's Office (ICO):

Summary incidents reported to the Information Commissioner's Office				
Date of incident	**Nature of Incident**	**Nature of data involved**	**Number of subjects potentially affected**	**Outcome of Incident**
November 2018 - Data Breach occurred **11th February 2019** – Identification a breach had occurred and Notification of Data Breach to the ICO	During a deep clean exercise within the a Trust Department it would appear that a ring binder file containing staff member "Statement of Fitness to Work" medical notes has have been inadvertently disposed with a) confidential waste or b) general waste	Personal Identifiable Information and Sensitive Personal Information	**250** staff members	**17th February 2019 –** Conclusion of ICO investigation – No enforcement action taken As a result of the incident, there was a review into the management and storage of statement of fitness to work documentation and a number of changes to practice implemented

Further ongoing actions include:

- A review of the Trust's Records Management Policy, with the recommendation that the policy be split into 2 separate policies; Corporate Records Management and Patient Records Management.

- A schedule of Confidentiality/Data Protection Walkarounds has been commenced to provide assurance Departments are following and applying the Trust's Information Governance and Information Security related policies and procedures

A summary of incidents requiring notification to the Information Commissioner's Office since 2016 is detailed below:

Year	Number of ICO Reportable Incidents
2016 - 2017	**1**
2017 – 2018	**0**
2018 – 2019	**1**
20019 - present	**0**

On each occasion the Information Commissioner's resolved that they would not take any further action as a result of the breach

4. Information Governance/Data Security & Protection Toolkit Annual Submissions

The Data Security and Protection Toolkit replaced the previous Information Governance toolkit during April 2018

The Data Security and Protection Toolkit is an online self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

For 2018-2019 the Toolkit comprises of 148 requirements which are either met or not met. Of these, 101 are mandatory and 47 are currently not mandatory. Organisations are expected to achieve 'Standards Met' where they have provided evidence for all the mandatory evidence items and confirmed the assertions

Information Governance Toolkit Annual Submissions (up until March 2018)				
Assessment	**Stage**	**Overall Score**	**Grade**	**MIAA Information Governance Toolkit Audit Assurance**
Version 8 (2010-2011)	Published	78%	Satisfactory	N/A
Version 9 (2011-2012)	Published	78%	Satisfactory	Limited Assurance
Version 10 (2012-2013)	Published	80%	Satisfactory	Limited Assurance
Version 11 (2013-2014	Published	80%	Satisfactory	Significant Assurance
Version 12 (2014-2015	Published	80%	Satisfactory	Significant Assurance
Version 13 (2015-2016	Published	80%	Satisfactory	Significant Assurance
Version 14. (2016-2017)	Published	80%	Satisfactory	Significant Assurance
Version 14.1 (2017-2018)	Published	83%	Satisfactory	Significant Assurance

Data Security & Protection Toolkit Annual Submissions (from April 2018)						
Assessment	**Stage**	**Requirement Type**	**Total Number**	**Complete**	**Not Complete**	**MIAA Information Governance Toolkit Audit Assurance**
2018-2019	Published	Mandatory	101	101	0	Substantial Assurance
		Non - Mandatory	47	20	27	

To fully comply with the Trust's NHS England Standard Contract, General Conditions 21.6 which states that the Trust must ensure that its NHS Data Security & Protection Toolkit submission is audited in accordance with Information Governance Audit Guidance the Trust's internal auditor, Mersey Internal Audit Agency (MIAA) complete an annual review and assign an assurance level against the Trust's Data Security & Protection Toolkit compliance. This assurance level is show in the table above.

5. Training

In the reporting period the Caldicott Guardian completed the following role specific training:

- Annual Data Security/Information Governance Awareness training – December 2019
- CPD Accredited Caldicott Guardian Training Course (Stay Compliant Ltd) – March 2019

Appendix A – Caldicott Function Plan 2018 – 2019

Trust Wide Strategy

CALDICOTT FUNCTION PLAN

2018-2019

Name and designation of policy author(s)	Andrew Ivers, Information Governance Manager (Data Protection Officer)
Approved by (committee, group, manager)	Kate Greaves- Associate Director of Quality
Approving signature	Electronic approval received
Date approved	19th November 2018
Review date	November 2019
Review type (annual, three yearly)	Annual
Target audience	All staff
Links to other strategies, policies, procedures	Data Protection & Confidentiality Policy Information Governance Policy Records Management Policy Registration Authority Policy & Procedure Information Governance Communications & Training Strategy Records Management Strategy Caldicott Approval Procedure Information Governance Framework Information Sharing Agreement Template Cheshire & Mersey Information Sharing Code of Practice
Protective Marking Classification	Internal
This document replaces	V1.0

Consultation:

	Authorised by	Date Authorised	Comments
Impact Assessment	N/A	N/A	N/A
Fraud Assessment	N/A	N/A	N/A

Circulation/Dissemination:

Date added into Q-Pulse	20th November 2018
Date notice posted in the Team Brief	20th November 2018
Date document posted on the intranet	20th November 2018

Version History:

Date	Version	Author name and designation	Summary of main changes
June 2017	1.0	Andrew Ivers, Information Governance Manager	New Document
May 2018	2.0	Andrew Ivers, Information Governance Manager (Data Protection Officer)	Reviewed and updated to incorporate new General Data Protection Regulations, Data Security Standards and Data Security and Protection Toolkit

Contents

1.0 Introduction

The 1997 report of the Review of Patient-Identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report), made a number of recommendations for regulating the use and transfer of patient identifiable information between NHS organisations in England and to non-NHS bodies. The Caldicott Committee's remit included all patient identifiable information passing between organisations for purposes other than direct care, medical research, or where there was a statutory requirement for information. The aim was to ensure that patient identifiable information was shared only for justified purposes and that only the minimum necessary information was shared in each case.

The recommendations of the Caldicott Committee defined the confidentiality agenda for NHS organisations. A key recommendation was the appointment in each NHS organisation of a "Guardian" to oversee the arrangements for the use and sharing of patient identifiable information. Another recommendation was that every use or flow of patient identifiable information should be regularly justified and tested against the principles developed in the report. These principles can be found in Appendix A.

A further review was commissioned during 2013 and again chaired by Dame Caldicott to look at the balance between the need to share patient or service user identifiable information and protecting confidentiality. This resulted in a report entitled '*Information: To share or not to share?*' the addition of a seventh principle about information sharing and a further 26 recommendations.

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

2.0 Key Caldicott Responsibilities

2.1 Strategy & Governance

The Caldicott Guardian should champion confidentiality issues at board/senior management team level, should sit on an organisations Information Governance Board and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

2.2 Confidentiality & Data Protection Expertise

The Caldicott Guardian should develop knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott Function but also on external sources of advice and guidance where available.

2.3 Internal Information Processing

The Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisations Caldicott function are detailed in the Data Security and Protection Toolkit.

2.4 Information Sharing

The Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

3.0 The Caldicott Function

3.1 Data Protection

3.1.1 The Caldicott Guardian at The Clatterbridge Cancer Centre NHS Foundation Trust will:

- ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented;
- ensure compliance with the principles contained within the Confidentially: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training;
- ensure completion of any confidentiality and data protection assurance requirements contained within the Data Security and Protection Toolkit, contributing to the annual assessment;
- update a Caldicott log (see Appendix B) with items related to confidentiality and data protection where advice, sign-off, etc. has been given.

3.1.2 In relation to information disclosures, the advice of the Caldicott Guardian will be sought prior to making any statutory or public interest disclosure.

3.1.3 The Caldicott Guardian will work with Associate Director of Quality and the Information Governance Manager (Data Protection Officer) on confidentiality issues.

3.2 Policy and Procedure Development

The Caldicott Guardian is an integral part of an Information Governance Board which promotes a unified approach to Information Governance and which supports the overall Information Governance infrastructure. Part of this involves approval and reviewing of policies and procedures relating to data protection and confidentially requirements.

3.3 Records Management

The Information Governance Manager and Administration Services Lead will consult with the Caldicott Guardian to ensure that the organisation's Records Management Strategy and Records Management Policy adhere to current Department of Heath guidance and protocols on confidentiality.

3.4 Information Security

The Trust's Information Security Manager, when necessary, will escalate security risks to person identifiable and confidential patient information to the Caldicott Guardian. The Caldicott Guardian will monitor incident reports indicating loss of confidential information and will have accountability for ensuring breaches of confidentiality are investigated and ensuing action plans are delivered to facilitate organisational learning.

3.5 Information Sharing

The Caldicott Guardian will agree and sign off Information Sharing Protocols/Agreements on behalf of the organisation, outlining rules relating to the sharing of information with other organisations and provide guidance to staff in relation to sharing confidential information. The Trust adopts a 2 layered approach:

Overarching Cheshire & Mersey Information Sharing Commitments – This is a high-level agreement, in principle, to share information with partner organisations. Information Sharing Commitment documents are approved and signed by organisational Chief Accountable Officers (Chief Executives).

Information Sharing Agreements - Specific detailed Information Sharing Agreements which define specific purposes and processes by which information can and will be shared. These documents are approved and signed by the Caldicott Guardian.

3.6 Data Protection Impact Assessments

The Caldicott Guardian is responsible for ensuring that Data Protection Impact Assessments have taken appropriate care in assessing the effect on privacy with the patient or data subject in mind, that all uses of the personal data and/or sensitive information are appropriate, and that they have assessed and given appropriate sign off to those processes.

3.7 Registration Authority

The Caldicott Guardian is responsible for the overall governance of Registration Authority and Position/Role Based Access Control arrangements within the organisation.

3.8 Caldicott Approvals

The Caldicott Guardian will oversee all requests for the use and release of patient identifiable data to NHS and Non-NHS organisations and ensure the correct processes are carried out in accordance with the seven Caldicott principles.

Requests for information may come from a number of sources:

- Internal staff for e.g. medical students undertaking courses;
- Junior doctors, consultants, professors etc. undertaking research studies and service evaluations;
- Teaching hospitals;
- Clinical auditors who are undertaking service evaluations etc.

Examples of when Caldicott approval must be sought include:

- Proposals for medical research projects that intend to use patient identifiable information;
- Collecting information to create an information database/system for e.g. a local Trust system or national registration system;
- Serious information disclosures to the Police, the Courts etc.

4.0 Knowledge, Education & Training

It is necessary to ensure that the Caldicott Guardian has adequate confidentiality and data protection skills, knowledge and experience to successfully co-ordinate and implement the confidentiality and data protection work programme. To enable them to fulfil their role of Caldicott Guardian, the nominated individual, will be required to complete training modules as outlined in the Information Governance Communications & Training Strategy on an annual basis.

In addition the Caldicott Guardian may attend Caldicott Guardian meetings arranged by the UK Caldicott Guardian Council. Conferences, seminars and other learning events provide other opportunities for knowledge transfer and continuing personal development.

5.0 Monitoring

The Caldicott Function Plan will be monitored through the Information Governance Board and reported through the Data Security and Protection Toolkit submission.

6.0 Review

This plan will be reviewed annually in line with Data Security and Protection Toolkit requirements or where changes occur with legislation or national policy.

7.0 References

7.1.1 Books

N/A

7.1.2 Journals

N/A

7.1.3 Internet

Information: To Share or Not To Share? The Information Governance Review

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

UK Caldicott Guardian Council

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

A Manual for Caldicott Guardians

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

Data Security and Protection Toolkit

https://www.dsptoolkit.nhs.uk/

8.0 Appendices

Appendix A

CALDICOTT PRINCIPLES

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or external to the organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the Caldicott Guardian.

Principle 2: Don't use personal confidential data unless 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 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 patient identifiable information 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 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: Understand and 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