University Hospitals of Leicester NHS
NHS Trust

Confidentiality Audit Procedures

& Policy

Approved By:	Policy & Guideline Committee
Date of Original Approval:	15 April 2016
Trust Reference:	**B10/2016**
Version:	2.0
Supersedes:	1.0 – April 2016
Trust Lead:	Saiful Choudhury, Head of Privacy
Board Director Lead:	Andrew Carruthers – Chief Information Officer & Senior Information Risk Officer
Date of Latest Approval	29 July 2022 – Policy and Guideline Committee
Next Review Date:	May 2026

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

This version covers what the audit is in more detail. Who the audit is applicable to and how it fits in with our aims.

KEY WORDS

Audit, Confidentiality, Information Governance, monitoring

1 INTRODUCTION AND OVERVIEW

1.1 The need to monitor access to confidential information has become important because we are using more NHS systems. With the large number of staff using these systems it is important that access is strictly monitored and controlled.

1.2 The aim of this policy is to assist staff in carrying out confidentiality audits and understand their responsibilities when auditing personal confidential data.

1.3 The movement of confidential information through these systems poses the threat of information falling into the hands of individuals who do not have a legitimate right of access to it.

1.4 Failure to have adequate controls to manage and safeguard confidentiality may result in a breach of that confidentiality. Therefore breaching the requirements of Caldicott, the Data Protection Act 2018, General Data Protection Regulation 2016, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

1.5 These procedures provide an assurance mechanism by which the effectiveness of the controls within University Hospitals of Leicester NHS Trust (UHL) are audited. Audits will highlight areas for improvement and concern. The audit will allow recommendations for improved control and enable management of confidentiality within UHL.

1.6 This work forms part of the Trust's overall information governance assurance framework and meets requirements within:

- The NHS information Governance Toolkit
- NHS Digital Data Security and Protections Toolkit
- The NHS Confidentiality Code of Conduct
- Guide to Confidentiality in Health and Social Care
- Registration Authority arrangements for NHS Organisations

2 POLICY SCOPE

2.1 This policy applies to all staff working for, or on behalf of the Trust (UHL). It also applies to any agency workers, students and volunteers whilst on placement with the Trust.

3 DEFINITIONS

3.1 **CQC**: is the independent regulator of all health and social care services in England. Its job is to make sure that care provided by hospitals, dentists, ambulances, care homes and services in people's own homes and elsewhere meets government standards of quality and safety.

3,2 **Information Asset**: An information asset is a body of information that is defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

3.3 **Information Asset Owners (IAOs)**: is a senior member of staff who is the nominated owner for one or more identified information assets within the service/Trust.

3.4 **Personal Confidential Data:** for the purpose of this guidance, is defined as any information about a person which would allow that person to be identified.

4 ROLES AND RESPONSIBILITIES

4.1 **Senior Information Risk Owner (SIRO):** The SIRO takes ownership of the organisation's information risk policy and acts as an advocate for information risk on the Executive IM&T Board. The SIRO for the Trust is the Chief Information Officer for IM&T, who is also the Executive Lead for the policy. The SIRO will be updated with finding of the confidentiality audits and will receive copies of all reports

4.2 **Medical Director (Caldicott Guardian):** The Caldicott Guardian will ensure that confidentiality audits of security and access arrangements within each area are completed on a regular basis.

4.3 **Information Governance Steering Group:** Information Governance Steering Group (IGSG) is the Designated Committee for this policy

4.4 **Privacy Unit:** The Privacy unit will be responsible for ensuring that access to confidential information is audited within the Trust. Ensuring that reports produced from the Clinical Systems and other local computer systems are reviewed and followed-up.

4.5 **Head of Privacy (Data Protection Officer):** The Head of Privacy has lead responsibility for Data Protection, Confidentiality and the Data Security & Protection Toolkit within the Trust. Ensuring staff have access to the up to date guidance on keeping personal information secure; ensuring that evidence is made available to support the attainment levels reported to Connecting for Health; reviewing and evaluating IG arrangements and communicating changes in assessment/guidance across all functional areas; The Head of Privacy should be contacted in the event of IG queries or incidents.

4.6 **Information Asset owners (IAOs):** Information Asset owners take overall responsibility for one or more assets. The IAO is responsible for reporting any breaches that happen with their assets to the SIRO. The IAO is required to identify and mitigate any risks to the asset. The IAO decides which users have access to the asset, ensuring that staff are aware of their responsibilities with regard to confidentiality of information by completing appropriate mandatory Information Governance Training. The IAO is responsible for auditing their assets annually.

We are now piloting a structure where there will be 100 or so Senior Information Asset Owners (SIO) who will have Information Asset Owners reporting to them. The SIAO will report to SIRO (with delegated power to Data Protection Officer) to collate this.

5 POLICY STATEMENTS

5.1 Confidentiality Audit Approach

All departments that have information assets will be required to carry out Confidentiality audits. This should be carried once a year (annually). Audit results will be maintained by Privacy on the Information asset register. Major Assets, smaller bits of paper that have temporary use are not to be reported, this is information that is constantly being maintained and used and stored (refer to definition of assets).

Trust wide systems do not need to be audited.

Privacy Unit will assist the first audit. Audits will be automated in Year 2 onwards where it auto populates the register rather than a spreadsheet as it is currently.

Please see appendix 1 for audit checklist.

5.2 Additional circumstances when an audit may be required are, for example;

- A potential breach of confidentiality
- A change of Information Asset Owner
- Data being migrated to another system
- Major change to an Information Asset, etc.

5.3 Confidentiality audits can be carried out in a number of ways;

- Interviews with staff using structured questionnaires
- Notified audit visits with structured questionnaires
- Spot checks at random work areas
- Audit carried out by the Information Asset Owner on electronic records
- Registration Authority (smartcard usage) enhanced reporting facilities

5.4 The information within the audit will contain at minimum any examples of or including the following information:

- Failed attempts to access confidential information inappropriately;
- Repeated attempts to access confidential information inappropriately;
- Successful access of confidential information by unauthorised persons;
- Evidence of shared login sessions/passwords

Reports of the findings from annual audits will be presented to the IG Steering group annually.

5.5 Areas to be audited include:

a) Security applied to manual files e.g. storage in locked cabinets / locked rooms

b) Arrangements for recording access to manual files e.g. tracking cards.

c) Evidence that checks have been carried out to ensure that the person requesting access has a legitimate right to do so

d) The use of and disposal arrangements for post it notes, notebooks, other temporary recording material

e) Retention and disposal arrangements

f) Confidential information sent or received via email, security applied and email system used

g) Information removed from the workplace – has authorisation been gained either for long term or short term removal in line with trust policy.

h) Security arrangements applied i.e. transportation in secure containers

i) The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information

j) Security applied to laptops, compliance with UHL Information Security Policy

k) The use/availability of encrypted memory sticks

l) Passwords being used within the area being audited

m) Confidentiality audit results will be collected and recorded for analysis and future reporting. Reports will be discussed at the IGSG annually and will highlight any areas for improvement and learning.

n) If a breach or any risks of breaches in personal confidential data are identified from the confidentiality audits, matters will be reported and investigated through the UHL Incident and Accident Reporting Policy (A10/2004) and

Disciplinary Policy (A6/2004) where appropriate.

5.6 Choosing Appropriate Auditors

Confidentiality audits will be managed by those who have received IAO training. It is department responsibility to determine who is best to collate this information based on the training pre requisite. It may be more than one person that has received the training and could be job share depending on size of department and number of systems managed. All department specific systems are a must. Trust wide systems do not need to be reviewed.

It is recommended that the individuals selected have a good knowledge of the requirements of:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- 7 Caldicott Principles etc.

Auditors should have the ability to express concerns and ideas effectively in verbal and written form.

The quality of the confidentiality audits should:

- Demonstrate an objective and responsible approach
- Process sound judgment, excellent analytical skills and tenacity
- Demonstrate a rational approach in diverse situations
- Demonstrate the ability to understand complex processes
- Demonstrate the ability to understand the role of the area being audited in UHL as a whole

5.7 Audit Method

5.7.1 The audit should be carried out using Appendix 1.

5.7.2 This can be through a series of interviews with Local Managers.

5.7.3 The interview should be both informal and relaxed this will encourage the interviewee to be more open with answering questions.

5.7.4 Interviews can be conducted either on a one to one basis, as a focus group, or a mixture of the two.

5.7.5 During the interview or focus group meeting, the interviewer should take brief notes which can be written up following the meeting. It is important that the individuals involved in the interview process do not feel intimidated as this could impact on the efficacy of the audit.

5.8 Re audit method

The annual re-audit will be based on the outcome of the previous year’s audit and should include any new information assets that may have been introduced in that time.

5.9 Reporting

5.9.1 A formal report by the auditor should be provided to the department or area being audited. This can be valuable to the department or area, as it provides information as to their compliance with confidentiality requirements..

5.9.2 Where non-compliance is observed, this should be recorded as soon as possible. The report should include all the facts and refer to any relevant evidence.

5.9.3 The detail recorded should include:

- An outline of what was observed
- where it was observed, who was involved
- the date of the observation and why it was considered to be non-compliant.

5.9.4 Each non-compliance observed should have an associated recommendation which should be discussed and agreed with the Service Lead. Each recommendation should also include a target date for completion and a named individual who will be responsible for ensuring that the recommendation is implemented.

5.9.5 Non-compliance can fall into one of two categories:

- Major Non-Compliance: this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequence For example, Patient Identifiable Data (PID) being left in public view, passwords to logins in full public view,
- Minor Non-Compliance: these could include one off occurrences of non-compliance, there is little risk of the non-compliance causing more than a minor irritation. For example, discussing patient in open area that is unavoidable, not locking doors.

Where a number of minor instances of non-compliance occur in the same area or department it may indicate a more serious problem. If this is the case, these instances of non-compliance should be combined into a major non-compliance.

There may be instances where the auditor is concerned by what has been observed, but the instances are not actual non-compliances. In this case the auditor can make recommendations for improvements to be made to practice in order that potential problems do not occur.

6 AUDIT FREQUENCY

Audits are required to be carried out annually. Privacy Unit will maintain the list of confidentiality audits and will notify departments of the anniversary of their audit 3 months before it is due. Privacy Unit will assist in collating information the first audit and the IAO will re-audit (spot check) annually to ensure that remediation actions are working.

7 EDUCATION AND TRAINING REQUIREMENTS

It is recommended that individuals selected as Auditors receive appropriate training prior to commencing the audit process; however, this is not a mandatory requirement. Training is part of essential/mandatory Level 3 Cyber Security Training.

8 PROCESS FOR MONITORING COMPLIANCE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
Review of Policy	Head of Privacy			
CQC Outcome 17	Head of Privacy	DS&P toolkit	Quarterly via the IGSG Annually via the Data Security and Protection Toolkit	Information Governance Steering Group Audits should be submitted to: Infogov@uhl-tr.nhs.uk
DS&P Toolkit	Head of Privacy	DS&P toolkit	Quarterly via the IGSG Annually via the Data Security and Protection Toolkit	Information Governance Steering Group Audits should be submitted to: Infogov@uhl-tr.nhs.uk
DS&P Toolkit	Head of Privacy	DS&P toolkit	Quarterly via the IGSG Annually via the Data Security and Protection Toolkit	Information Governance Steering Group Audits should be submitted to: Infogov@uhl-tr.nhs.uk

9 EQUALITY IMPACT ASSESSMENT

The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

10 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

This policy is in support of the following;

- Information Governance Toolkit requirements
- Data Security and Protections Toolkit 2018
- Data Protection Act 2018
- General Data Protection Regulation 2016
- Caldicott Guardian Requirements (revised 2013)

- Information Governance Policy (B4/2004)
- Information Security Policy - A10/2003

11 Process for Version Control, Document Archiving and Review

The UHL Information Governance Steering Group are responsible for keeping this policy up to date.

The policy will be reviewed every three years or sooner if there is any significant change in legislation or if a technology that has not been used at UHL is to be employed

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts PAGL system

APPENDIX 1 – GOLD STANDARD AUDIT CHECKLIST

Are You GDPR Compliant? Gold Standard Governance Audit Checklist: If you can answer 'yes' to all these questions, and have evidence to support this, the department can demonstrate GDPR compliance.			
Department Name is:			
Person completing this checklist's name and job role is:			
Questions		**Yes/No/Unsure (Contact Privacy Unit)**	**Comments/ Evidence-** Add a link to any supporting evidence.
Key Personnel:			
Q.1	All Staff on this department know that the Trust's Caldicott Guardian is the Medical Director, the Senior Information Risk Owner is the Chief Information Officer and the Data Protection Officer is the Head of Privacy.		
Q.2	There is an identified Information Asset Owner for each Information Asset (database, system, cabinet, diary, that holds PCD) held by this department. This individual is responsible for informing the Privacy Unit of Information Risks and any Confidentiality Breaches that may occur.		
What Personal Confidential Data (PCD; Information that identifies an individual) is held by the department?			
Q.3	This department keeps a record of where all PCD of **staff (including volunteers, bank staff and locums)** is stored, and what it is. This includes electronic and paper storage.		
Q.4	This department keeps a record of where all Personal Confidential Data (PCD) of **patients** is stored, and what it is. This includes electronic and paper storage, and includes electronic systems, filing cabinets, diaries and more.		
Q.5	All of the electronic systems that this department uses have been added to the Information Asset Register held centrally by the Privacy Unit. *(Example: SYSY system; holds patient data; Information Asset Owner is Jane Bloggs)*		
Q.6	Any paper filing systems that the department uses to store PCD are included on the Information Asset Register held centrally by the Privacy Unit. *(Example: x2 Filing Cabinets holding paper records of Oncology staff, located at XXXXX, IAO is Joe Bloggs)*		
Q.7	This department is aware of and adheres to the retention schedules detailed in the Records Management Code of Practice here:		

	(LINK below)		
	https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016		
Q.8	This department annually reviews what PCD it keeps, to audit what must be kept, what can go into off site storage and what can be destroyed. Clinical data is reviewed by a clinician.		
Q.9	All staff in the department have read the Trust's Privacy Notice. Link below.		
	https://www.leicestershospitals.nhs.uk/aboutus/about-this-website/data-protection/		
Q.10	Any work that this department does that includes using PCD is covered by the Trust's public Privacy Notice.		
Q.11	There are physical controls (locked doors, locked cabinets, electronic badge readers) that prevent unauthorised access to PCD held by this department. All staff ensure that these are fully utilised to keep the data safe.		
Lawful Basis:			
Q.12	Is there substantial public interest in completing the work that your department does? This includes purposes of improving public health, scientific research purposes and ensuring high standards of quality and safety of healthcare services and medicinal devices and products.		*Think about the public health consequences if the department could no longer complete processing activities.*
Q.13	Is this work necessary for the purposes of preventative medicine, or for treatment/management of health or social care services? This includes for the management, recruitment and employment of healthcare staff.		
Q.14	If the department handles patient data- Is the processing of patients' PCD carried out for the purposes of providing care directly to the patient? *Some of the activity may fall into this category, some may not. An example of processing that is not for direct care is sharing patient level information with other organisations.*		*If some of the activity is not done to provide direct care, for that activity to be compliant you must be able to answer Yes to Question 14 and 15 for it.*
Q.15	Special Category' data means information about an individual's health, mental health, race/ethnicity, political opinions, religious or philosophical beliefs, sexual health or sexual orientation. It includes the processing of images and biometric or genetic data.		*If 'Yes', to be compliant the work MUST be necessary for the purposes of preventative medicine, or for*

	Does your department process this? If no such data is processed, answer 'Not Processed' to this question.		*treatment/management of healthcare services.*
If there are processing activities that the department carries out that cannot be legally justified by the conditions above, contact the Privacy Unit on 0116 258 8537 or infogov@uhl-tr.nhs.uk			
Staff Responsibilities and Awareness:			
Q.16	At least 95% staff on this department have been trained in Data Protection and Cyber Security, whether this is through HELM, face to face or through the Workbook, in the last 12 months.		
Q.17	All staff ensure that PCD is always sent securely: using UHLEncrypt for emails outside of uhl-tr.nhs.uk email addresses and ensuring that the correct message is going to the correct person.		
Q.18	All new staff attend the mandatory Trust induction which contains a section on Data Protection and Cyber Security.		
Q.19	All staff challenge those attempting to enter the department if they do not have appropriate identification.		
Q.20	The electronic systems used on this department can audit who has accessed what data and when.		
Q.21	The systems used on this department require each user to have their own login credentials. There is a role based hierarchy of what each user can access.		
Q.22	Each staff member knows not to ever share their login credentials or to log in for another person. Credentials are never left where they may be used by others, i.e. written down and attached to a computer monitor. Disciplinary action can be taken for breaches.		
Q.23	Human Resources and Information Management and Technology are informed when a staff member moves departments, leaves or starts a position on this department. This allows user accounts and access to systems to be altered to reflect changes in a timely manner.		
Q.24	All staff on this department know how to use Datix, or who they can report to in order to have a Datix incident raised, to report confidentiality breaches and near misses.		

Q.25	All staff on this department know how to continue doing the critical parts of their jobs if a data security incident was to prevent technology from working in the organisation.		
Q.26	All staff have read and understand the Trust's Data Protection and Confidentiality Policy, Information Security Policy, Control of Access to Electronic Systems Policy and the Email and Internet Policy and adhere to them, alongside the local/departmental procedures and policies.		
Q.27	Departmental processes are reviewed at least annually to identify and improve processes that have caused confidentiality breaches or near misses. Participation is comprehensive, and action is taken to address problems.		
Electronic Systems:			
Q.28	All software used by this department is patched as required and updated regularly.		
Q.29	All Trust laptops and other devices are connected to the Trust network (i.e. Brought onto the premises and connected to the WiFi) on a regular basis to ensure they receive updates.		
Q.30	All of the electronic systems used by this department are supported by the Trust's IM&T Department. If not, arrangements have been made with IM&T to allow another supplier to support the system.		
External Suppliers and Data Processors:			
Q.31	This department keeps a list of suppliers external to the Trust that handle PCD, the products and services they deliver, their contact details and the contract duration. There must be a contract in place with each supplier that contains clauses required by GDPR.		*Templates are available from the Privacy Unit on 0116 258 8537 or infogov@uhl-tr.nhs.uk*
Q.32	Each supplier contract contains clauses about Data Protection and Cyber Security and is compatible with the General Data Protection Regulation 2016 and the Data Protection Act 2018.		
Q.33	Supplier contracts are maintained and are reviewed when legal changes occur and in good time before the expiration date is reached.		
Q.34	All of this department's external suppliers that handle PCD have given assurance of their preparedness for GDPR and are registered with the Information Commissioner's Office.		
Q.35	All external suppliers providing services to this department have completed an Information Governance Toolkit, or a Data Security and		

	Protection Toolkit.		
Q.36	All staff working on this department understand that if a new system or some new software is to be purchased, IM&T will need to be consulted and potentially a Data Protection Impact Assessment may need to be undertaken before processing any PCD.		