Humber Teaching
NHS Foundation Trust

INFORMATION GOVERNANCE IT FORENSIC INVESTIGATION AND CONFIDENTIALITY AUDIT PROCEDURES

Document Reference	Proc453(IG)
Version Number	1.4
Author/Lead **Job Title**	Tracey O'Mullane IG Officer
Lead Director name	Peter Beckwith Senior Information Risk Owner
Consultation	
Date of Last Changes (This Version)	4 October 2023
Date of Next Review	October 2026
Name of approving group **Date of approval**	Information Governance Group 4 October 2023

VALIDITY – Procedures should be accessed via the Trust intranet to ensure the current version is used.

CHANGE RECORD

Version	Date	Change details
		Policy
1.00	*06/06/2011*	
1.01	*03/09/2012*	*Reviewed, changes approved by IG Committee 18 July 2012* • *Title changed from Information Governance & IT Forensic Policy to Information Governance IT Forensic Investigation Policy (Applicable to all services)* • *The procedure to monitor access to confidential patient information has now been included in the above policy and should be removed from circulation. Link http://intranet.humber.nhs.uk/monitor- access-to-confidential-patient-information-procedure.htm* • *The guidance for privacy officer has been removed and a link inserted into the policy which reduces the pages from 48 to 11. Duties and responsibilities have been updated. System audit activity is further detailed within the policy.*
2.0	*July 2016*	• *Rewrite of introduction, scope and policy statement* • *Insertion of Senior IT Desktop Engineer role in audit for employee computers and files.* *Expanded to include other Trusts systems 5.2. SystmOne, 5.3 PC MIS and 5.4 SCR and 5.5 SmartComs call Recording.*
		Procedure
1.0	*Oct 2016*	*Reviewed, major rewrite and changed from a policy to a procedure. Changed the Title to Information Governance IT Forensic Investigation and Confidentiality Audit Procedure*
1.1	*Sept 2019*	• *Reviewed against the new Data Protection Legislation. Minor changes* • *Updated the Trust's name.* • *Changed the SIRO Lead from Director of Nursing to Director of Finance.* • *Removed the role of Deputy Director of Governance and Patient Experience.* • *Added the role of the Caldicott Guardian.*

		• *Added the deputising roles in the absence of the SIRO and Caldicott Guardian.* • *Updated the reference defining an appropriate health professional from Statutory Instrument 2000/413 to the Data Protection Act 2018* • *Updated the IG Incident reporting reference to the Guide to Notification and Reporting of Data Security Incidents* *Changes made to the Head of IT responsibilities to include next steps action.*
1.2	*Sept 2020*	• *Update to Human Resources section in relation to details of the purpose of the investigation or persons involved should only be shared with Head of IT or the IT Operations Manager.* • *Addition of section on ESR and audit of the system at Appendix 1.* • *Procedure updated to Trust format* *Links within the procedure updated*
1.3	*Jun 2021*	*Add section on Logging.*
1.4	*October 2023*	• *Formatted to the trust's procedure document template.* • *Minor changes – updates to job titles, changes of team names* • *Removal of Section 7 Bribery Act section* • *Removal of Care Records Guarantee information at section 6, as it is no longer referenced or available on NHSE website* • *Call recording section updated to include reference to UK GDPR* *SAR section updated to reference staff SAR* *Approved at Information Governance Group (4 October 2023).*

Contents

1. PURPOSE

This procedure sets out how the Trust aims to maximise its ability to gather and preserve electronic data for the purposes of any criminal or disciplinary investigation.

Forensics may include evidence in the form of log files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that may be collected in advance of an event or dispute occurring. These types of audits are performed by the IT Services Team.

Confidentiality audits are for the purpose of monitoring access to clinical systems. They act as a deterrent to unauthorised activity and support subject access requests, investigations and complaints. These types of audit are performed by the Privacy Officer(s) in the Information Governance Team. This procedure details the documented confidentiality audit processes for each key Information Asset (see Appendix 1)

2. INTRODUCTION

Humber Teaching NHS Foundation Trust approved the introduction of IG forensic readiness into the business processes and functions of the Trust. Forensic readiness is the ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.

Computers may constitute a 'scene of a crime', for example with hacking[1] or denial of service attacks[2] or they may hold evidence in the form of emails, internet history, documents or other files. It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata[3]' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed, and which user carried out these actions

This should maximise its potential to use digital evidence whilst minimising the costs of investigation.

Good practice requires all organisations to have a documented confidentiality audit procedures in place. Confidentiality audits are different to forensic audits and are used to monitor and evidence legitimate access to clinical information.

3. SCOPE

This procedure applies to all employees of the Trust, including all staff seconded to the Trust, Contractors, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid on an honorarium.

[1] **Hacking:** modifying a computer in a way which was not originally intended in order to benefit the hacker's goals.
[2] **Denial of Service attack:** an attempt to prevent legitimate users of a computer system from having access to that system's information or services.
[3] **Metadata:** data about data. It can be embedded within files or stored externally in a separate file and may contain information about the file's author, format, creation date and so on.

4. DUTIES & RESPONSIBILITIES

The Chief Executive

Has overall responsibility for the effective implementation of this procedure.

The Senior Information Risk Owner (SIRO)

The Executive Director of Finance will be the senior manager with Board level responsibility for information governance and fulfil the role of the Trust's Senior Information Risk Owner (SIRO). The SIRO is responsible for coordinating the development and maintenance of IG & IT forensic investigation and Confidentiality Audit procedures and standards for the Trust. The SIRO is responsible for the ongoing development and day-to-day management of the IG & IT forensic and confidentiality audit procedure within the Trust's overall Risk Management Programme. The SIRO is jointly responsible for authorising an audit of a patient's record by the Privacy Officers.

Chief Information Officer

The Chief Information Officer will act as Deputy to the SIRO in relation to this procedure.

Caldicott Guardian

The Executive Director of Nursing, Allied Health and Social Care Professionals is the Caldicott Guardian who acts as the 'conscience' of the Trust, ensuring the formation we collect about our service users is used appropriately, legally and ethically, whilst maintaining confidentiality. The Caldicott Guardian is jointly responsible for authorising an audit of a patient's record by the Privacy Officers.

Deputy Director of Nursing, Allied Health and Social Care Professionals

The Deputy Director of Nursing Allied Health and Social Care Professionals will act as Deputy to the Caldicott Guardian in relation to this procedure.

Information Asset Owners (IAOs)

Shall ensure that IG & IT forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership'.

Head of IT

Shall be responsible for advising about the auditing of IT equipment and/or files of employees. The audit of IT equipment/files is at the request of Human Resources.The Head of IT will review for appropriateness and provide advice on next steps.

The next steps could include

- no action,
- requesting authority from CG or SIRO to proceed with audit,
- internal investigation with the support of the IT
- forwarding request to external agencies e.g Police. NHS Fraud etc.

Human Resources

Shall be responsible for requesting an investigation of an employee's IT equipment and/or files. The request will be submitted directly to the Head of IT or the IT Operations Manager. . Due to the potential sensitivity, details regarding the purpose of/ or persons involved in the investigation should not be shared with the IT Servicedesk. These details should only be shared with the Head of IT and/or the IT Operations Manager.

The IG Privacy Officer(s)

Shall be responsible for auditing key patient systems to provide pro-active and reactive reports on system alerts and adhoc system validation. Audit requests on who has accessed a patient's record will be initiated directly from the patient, Managers, or SI leads. Authorisation will be sought from the SIRO, Caldicott Guardian or DPO.

Privacy Officers will familiarise themselves with audit trails and other reporting tools across Trust systems to facilitate audits on key systems.

Information Governance Officers

Will provide training and awareness of the Privacy officer role within the Information Governance face-to-face training and auditing of systems.

Line Managers

Will ensure all new members of staff have attended information governance training at induction and understand the IG IT Forensic Investigations and confidentiality audit procedure.

5. EQUALITY & DIVERSITY

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust approved EIA. The assessment indicates that there is little or no evidence/concern that the policy will have a differential impact on any of the equality target groups.

6. MENTAL CAPACITY

This is a non-clinical procedure therefore not relevant.

7. FRAUD

Where any fraud is suspected it is important that all staff comply with the Local Anti-Fraud, Bribery and Corruption Policy . All suspicions of fraud should be reported directly to the Director of Finance or Local Counter Fraud Specialist (LCFS) who is authorised to treat enquiries confidentially and anonymously. Staff should not investigate these matters themselves.

The Local Counter Fraud Specialist is contactable on 01482 866800, by email: nikki.cooper1@nhs.net, Further details are available on the Trust intranet Counter Fraud section.

Referrals of fraud can also be made to the NHS Fraud and Corruption Reporting Line (FCRL) which is a free phone number **0800 028 4060**, on line at **https://cfa.nhs.uk/reportfraud** or by email to nhsfraud@nhsprotect.gsi.gov.uk.

8. IMPLEMENTATION

This procedure will be disseminated by the method described in the procedure for the Development and Management of Procedural Documents.

This procedure is to be made available to all Trust staff on the Intranet and observed by all members of staff, both clinical and administrative. There will be an ongoing professional development and educational strategy as part of the Information Governance training and awareness of this procedure to accompany the implementation of this procedure. The implementation of this procedure requires no additional financial resource.

9. MONITORING & AUDIT

The procedure will be monitored through the quarterly reporting process to the Information Governance Group. All monitoring which highlights a breach of confidentiality will be reported to the member of staff's line manager and the Trust's Disciplinary Policies followed.

10. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

Related Documents

- Information Security and Risk Policy
- IT Internal Operating Procedures
- Managing SystmOne Alerts Standard Operating Procedure
- Standard Operating Procedure for Auditing Alerts
- Standard Operating Procedure for Recording Patient Calls
- Guide to the Notification of Data Security and Protection Incidents
- Disciplinary Policy

APPENDIX 1 – CONFIDENTIALITY AUDIT PROCEDURES

Good practice requires all organisations to have a documented confidentiality audit procedure in place. Confidentiality audits are used in the NHS to;

- Provide proof of monitoring internal controls to auditors.
- Provide reports on system activity to auditors.
- Act as a deterrent to unauthorised activity.
- Retrospective analysis of the patient data to identify cause and effect.
- Assist with investigations of data breaches or other suspicious activity.
- Provide analysis of user access/actions and modifications to patient and non-patient data. Detect when attempts are made to bypass security control.
- Support a complaint investigation.
- Support a request by the patient for a list of staff who have access their health record

Confidentiality audits are performed by the Trust Privacy Officer(s) If a confidentiality audit is required contact the Information Governance Team on 01482 477854 to discuss.

LOGS

The Trust uses network, servers and electronic systems (clinical and non-clinical) to support the business of the Trust. As each system is used it creates records called Logs. Logs provide a mechanism for automated tracking and reporting for review, audit, and compliance functions, alerting and analysis to identify potential hazards/threats. Access to the Trust's network, systems and communications are logged and monitored to identify potential misuse of systems or information, compliance functions, alerting/analysis to identify potential hazards/threats, and to support internal investigations.

The Trust's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Protect against unauthorized access
- Verify security procedures and access
- Verify system and operational security
- Comply with the Trusts policies and procedures
- Detect and prevent criminal or illegal activities

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions record and retain audit logging information to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed
- Systems and objects involved
- When the activity was performed
- Status (such as success vs. failure), outcome, and/or result of the activity

Log servers and documents shall be kept secure and only made available to authorised personnel for the purposes stated.

PATIENT CONFIDENTIALITY

Patient data is protected by Legitimate Relationships (LR). Only users who have an LR with a patient can see a patient's EPR (electronic patient record). Alerts are generated from Trust systems to the Privacy Officers when a user self-claims a legitimate relationship to access a patients record, when a user access a deducted record and when patient consent is overridden**.** The investigating officer will be able to self-claim an LR to carry out their investigation.

Inappropriate access to any clinical system is an information governance breach. It will be investigated and managed in line with the **Guide to the Notification of Data Security and Protection Incidents**, NHS England on behalf of the Department of Health.

Any IG breach which *scores Liklihood that harm has occurred* **3 or above** *and severity impact of* **2 or above** will be notified to the Information Commissioners Office.

If it is found that any Trust system is accessed inappropriately, disciplinary action will follow the Trust Disciplinary Policy.

The patient will be informed under the Duty of Candour.

KEY SYSTEMS

The key electronic patient clinical systems in the Trust are Lorenzo and SystmOne.
The Trust also uses PC MIS in the NHS East Riding Talking Therapies service and IAPTUS in the Ops COURAGE Veterans Mental Health and Wellbeing Service. The Trust also uses the Summary Care Record. The key electronic staff system in the Trust is the Electronic Staff Record.

1 LORENZO

Lorenzo is the clinical system mainly used by mental health service in the Trust. There are a number of audits available in Lorenzo.

Audit Event Reports are available within Lorenzo for use by the Privacy Officer.

Report Name	**Content description**
User Patient Access Audit Report	Care Activity events for the specified for the specified patient in date/time order.
Patients Accessed by Users Audit Report	Care Activity events accessed in Lorenzo, grouped by User and patient id, and sorted in date/time order
User Session Audit Report	Session start & end events, showing role, workstation details and session duration of each logged in user session
Hard Copy Audit Report	User, Workstation, Date and Time details for all print jobs executed in Lorenzo via logical printers.
Alerted Events Audit Report	Any alerted events grouped by User ID, and sorted by date/time/patient Alerted event examples are:- LR Self Claims, Override of a patients dissent to share information, breaking of Seals.
Application Configuration Audit Report	Configuration 'event' activity, grouped by User, sorted by date/time.
Chart Audit Report	For the patient event type e.g. IP/OP/Day care (optional), patient id (optional), User id (optional). Event activity showing workstation location and allows analysis of what type of events happen in which locations. Sorted by date/time

Lorenzo Audit Event Content Reports (AECR)

The AECR is a detailed report only available from the system supplier (Deadalus). The report provides details of structured data items that have been inserted, updated (both before and after) or deleted, in the Lorenzo database. The AECR is provided as an excel spreadsheet.

The Privacy Officer is responsible for:-
Validating the request for the AECR.
Compiling the returned data into a report for the requester.

If an AECR report is required a ticket must be raised via the IT Service desk to the system provider (CSC).

- The ticket will include;
  - Specific Trust
  - Patient NHS Number
  - Date Range
  - The NHS net account the AECR is to be sent to directly fromDedalus.

The AECR is used to identify what data has been changed in a patients record.

2 SYSTMONE

There is a local Privacy Officer role within each SystmOne Unit. Alerts are generated in the SystmOne Unit when a deducted (discharged) patient record is accessed. The local Privacy Officer will review and manage the alerts as set out in the Managing SystmOne Alerts Standard Operating Procedure The Trust Privacy Officer will perform all audits to support complaints and serious incident investigations.

3 PC MIS

PC MIS is the patient record system used by the Emotional Wellbeing Service. The Privacy Officer for PC MIS is the Team Manager who will perform an audit on request to support complaints, serious incident investigations or Subject Access Requests.
Security Reports identify who has accessed and referred the record to other agencies. Security Reports are performed by the Team Manager and the Senior Admin in the Team Managers absence. Clinical alerts are reviewed and investigated by the Clinical Supervisors.

4 IAPTUS

IAPTUS is the patients record system used by the Veterans Outreach service. The Privacy Officer role is performed by the Team Leader who will perform an audit on request to support complaints, serious incident investigations or Subject Access Requests

5 ESR

The Electronic Staff Record (ESR) is the primary HR and Payroll Management System for staff records. Change event reporting and access audit reports are available in ESR. Due to the potential sensitivity regarding the purpose of/ or persons involved in an investigation; a request for an audit to support a complaint, investigation or serious incidents should be submitted directly to the ESR & Workforce Manager.

Staff can export basic information (e.g. personal details, absence history, training record, total rewards statement) about themselves through ESR employee self-service. If a more detailed subject access is required a request would need to be submitted to the ESR & Workforce Team.

6 Summary Care Record (SCR)

The SCR is a nationally held summary of a patient's clinical history, long term conditions, end of life care information and demographic details sourced from the GP record. It enables a healthcare professional with a legitimate relationship to the patient to access relevant information with the patient's permission to view.from anywhere in England. The SCR can be accessed via web-based software, or directly through the electronic patient clinical system e.g. Lorenzo or SystmOne.

A record is kept of everyone who has accessed a SCR and the reasons for access. Privacy Officers can audit the records using the national care records service portal to identify who has accessed the record, investigate automated alerts, and to check that the access was for a legitimate reason.

7 Call Recording

Some Trust services recordcalls made into and out of the service where the feature is enabled. An appropriate senior Manager in each area that call recording is in use will be responsible for all aspects of call management as set out in the appropriate Team Call Recording SOP.

If a call recording is required for investigation, complaint or a subject access request. The Manager will be asked to provide a copy of the recoding.

8 Subject Access Request (SAR)

At the request of the patient, the Trust will provide a list of all staff who have accessed their health records and when they did so. Requests can also be made by third parties to support complaints, or investigations. If the audit trail is from a system that crosses organisational boundaries, this will be done in consultation with the organisations concerned.

Following an investigation or if the Trust become aware of a breach, the Trust will inform the patient if their records have been deliberately accessed without permission or good reason. The breach will be reported to the Information Commissioner's Office. This is a requirement of UK GDPR

The Access to Health Record Policy will be followed when releasing audit trail information to the service user. The full names of staff detailed on the record will be provided unless it is likely to cause serious harm to the member of staff's physical or mental health or condition. This decision will be made by the "Appropriate Health Professional" as defined in Data Protection Act 2018 Schedule 3, Part 2.

Staff can also make a subject access for their personal information. These will be managed by the appropriate team in line with the Data Protection for Employment Records Procedure or the Electronic Communications and Internet Acceptable Use Procedure.

APPENDIX 2 – EQUALITY IMPACT ASSESSMENT

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. **Document or Process or Service Name:** Information Governance IT Forensic Investigation and Confidentiality Audit Procedures (Proc453(IG))
2. **EIA Reviewer (name, job title, base and contact details):** Tracey O'Mullane, Information Governance Officer, Mary Seacole Building, 01482 477855

3. **Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other?** Procedure

Main Aims of the Document, Process or Service This procedure sets out how the Trust aims to maximise its ability to gather and preserve electronic data for the purposes of any criminal or disciplinary investigation. Confidentiality audits are for the purpose of monitoring access to clinical systems. They act as a deterrent to unauthorised activity and support, subject access requests, investigations and complaints. This procedure details the documented confidentiality audit processes for each key Information Asset
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group 1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed? Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	How have you arrived at the equality impact score? a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	Low	A web search has not identified any issues in relation to inequality to groups with protected characteristics. Forensic readiness is the ability to gather evidence in the form of log files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that may be collected in advance of an event or dispute occurring. Confidentiality audits are for the purpose of monitoring access to clinical systems. The above simply evidences an individual's actions. It is collected within the systems automatically, irrespective of any protected characteristics.

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental health (including cancer, HIV, multiple sclerosis)	Low	As above
Sex	Men/Male Women/Female	Low	As above
Marriage/Civil Partnership		Low	As above
Pregnancy/ Maternity		Low	As above
Race	Colour Nationality Ethnic/national origins	Low	As above
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	As above
Sexual Orientation	Lesbian Gay men Bisexual	Low	As above
Gender Reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	As above

Summary

Please describe the main points/actions arising from your assessment that supports your decision.

There is no evidence of potentially negative effect on groups with protected characteristics.

The gathering of evidence in the form of log files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that is collected. The confidentiality audits are for the purpose of monitoring access to clinical systems.

This data is collected within the systems automatically, irrespective of any protected characteristics.

EIA Reviewer: Tracey O'Mullane, Information Governance Officer

Date completed: 13 September 2023	Signature: T O'Mullane