NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Information Asset and System Audit Policy

Policy Number	**IG/Pol/005**
Target Audience	**All Staff**
Approving Committee	**Policy Approval Group**
Date Approved	**January 2014**
Last Review Date	**April 2018**
Next Review Date	**April 2021**
Policy Author	**Head of Information Governance**
Version Number	**3**

Applicable Statutory, Legal or National Best Practice Requirements	ISO/IEC 27001 Data Protection Act 1998 Data Protection Act (The Processing Sensitive Personal Data) 2000 Human Rights Act 1998 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

The Trust is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	Feb 12	IG Manager	For comments/approval
1.0	Feb 12	IG Sub Group	Policy Approval Group
1.1	Aug 13	IG Team	Review and minor amendments
1.1	Jan 2014	Policy Approval Group	Approved by Policy Approval Group
1.2	April 2016	Head of IG	Minor updates to roles and terminology
1.3	April 2016	Policy Approval Group	Approved subject to minor amendments to S. 1, 3, 6, 7.1, 8 & 9
1.4	April 2016	J. McCartney	Amendments completed, references updated
2	April 2016	D. Williams	Final chair approval
2.1	January 2018	IG Subgroup	Minor updates, name changes
2.2	February 2018	Library Services	References updated
2.3	March 2018	J. McKay	Minor amendments made to sections 1 and 3
2.4	April 2018	Policy Approval Group	Approved subject to minor amendments
2.5	April 2018	J. McCartney	Amendments completed
3	April 2018	S. Arkwright	Approved by chair action

Equality Impact Assessment completed	By: Jackie McKay	Date: 23/3/18

Contents

1 Introduction

Bridgewater Community Healthcare NHS Foundation Trust (thereafter the Trust) is committed to maintaining confidentiality in the use of all systems currently utilised across the Trust and mitigating any risks to its information assets. The protection of patient/staff and business confidentiality is of the utmost importance and therefore procedures will be adopted to reduce the risk of abuse/ inappropriate use/access to systems.

This policy outlines the requirement for the audit of systems containing patient/staff identifiable information and business sensitive information.

This policy outlines the assignment of responsibilities and the process by which access to the systems held by the Trust is audited so as to identify any unusual data activity. This includes audit of unusual data activity of Trust staff and other data processors and appropriate third parties.

It is necessary to have an Information Asset Register with appropriate Information Asset Owners (IAO's) who take responsibility for mitigating any risks to the Trust information assets. The Trust must also have in place appropriate audit measures for monitoring the use of those systems by Trust staff - see Appendix 3.

The Information Asset Register is held with the Information Governance (IG) Team.

The privacy of confidential information is of paramount importance and the Trust must ensure compliance with legal requirements including the Data Protection Act 1998, the forthcoming The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and Department of Health guidelines.

1.1 Objective

To ensure the confidentiality and quality of data held on Trust information assets.

1.2 Scope

This policy applies to all staff employed by the Trust and to staff employed by other organisations working on sites with assets managed by the Trust.

2 Definitions

The definitions applicable to this policy are as follows:

Senior Information Risk Officer (SIRO)	The SIRO is a Senior Management Board Member who is familiar with, and takes ownership of, the organisation's information risk policy and acts as advocate for information risk on the Board. The Director of Finance adopts this role within the Trust.

Information Asset	An information asset is a system that contains, stores, processes or transmits NHS or other UK Government information. Information assets can be electronic or hardcopy material, which includes paper records, microfiche, X-rays etc.
Information Asset Owners (IAO)	Information Asset Owners are senior Individuals who are involved in their Service Areas within the Trust. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
Information Asset Administrators (IAA)	Information Asset Administrators (IAA) ensures that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. Trust information assets may have more than one IAA.
Personal Information Content	Databases and data files Back-up and archive data Audit data Paper records (patient case notes and staff records) Paper reports
Software	Applications and System Software Data encryption utilities Development and Maintenance tools
Other Information Content	Databases and data files Back-up and archive data Audit data Paper records and reports
Hardware	Computing hardware including PCs, Laptops, PDA, communications devices e.g. blackberry and removable media
System/Process Documentation	System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Business continuity plans
Miscellaneous	Environmental services e.g. power and air-conditioning. People skills and experience. Shared service including networks and printers, computer rooms and equipment record libraries

Unusual Data Activity	Unusual data activity – may be defined, but is not exclusively defined, as any unauthorised viewing or modification of records or documents

3 Abbreviations

The abbreviations applicable to this policy are as follows:

IAO - Information Asset Owner

IAA - Information Asset Administrator

SIRO - Senior Information Risk Owner

IT - Information Technology

IG - Information Governance

SI - Serious Incident

PC - Personal Computer

GDPR - General Data Protection Regulation

EU - European Union

4 Other Relevant Procedural Documents

This policy should be read in conjunction with the following documents:

- ➢ Information Governance Policy
- ➢ Health Records Management Policy
- ➢ Information Security Policy
- ➢ Acceptable Use Policy
- ➢ Incident Reporting Policy

5 Roles and Responsibilities

5.1 Chief Executive

The Chief Executive, as the Accountable Officer, has overall responsibility for this policy and ensuring its effectiveness.

5.2 Senior Information Risk Officer (SIRO)

To comply with the definition above and the responsibilities set out in Appendix 1. The Director of Finance as SIRO has overall responsibility for reporting the outcomes of all conducted audits from the Information Asset Register to the Board.

5.3 Information Asset Owners

To comply with the definition above and the responsibilities set out in Appendix 2. They are responsible for reporting any unusual data activity to the SIRO via the IG Team and ensure that the appropriate procedures are followed to investigate and log the incident.

5.4 Information Asset Administrators

To comply with the definition above, they are responsible for conducting investigations into any instances of unusual data activity, as directed by the Information Asset Owner, and for reporting the investigation and its outcomes to the Information Asset Owner.

5.5 Information Governance Team, Assistant Directors and Clinical Managers

The Information Governance Team, Assistant Directors and Clinical Managers are responsible for the dissemination of this Policy and updating the Information Asset Register. They will also ensure the SIRO, IAO's and IAA's are supported in their duties as detailed in the Appendices. The Head of Information Governance will support any investigation outlined below and is responsible for maintaining the Information Asset log as well as a log of unusual data activity.

The Head of Information Governance will support the SIRO as appropriate.

5.6 Clinical Implementation Manager

The Clinical Implementation Manager is the designated Privacy Officer and is responsible for logging and monitoring the course and outcomes of any investigations into unusual data activity on SystmOne or any other electronic system.

6 Equipment List

Not applicable.

7 Process

The process for audits of the Information Asset Systems is as follows: see appendix 3

- IAA's will run regular audits at random depending on the type of system. The IAA's will analyse the results of these audits to establish whether there has been any unusual data activity in relation to personal data.

- The results will be reported to the Service Lead and the IAO where necessary or different.

- The Service Leads and IAAs, supported by the Clinical Implementation Manager and Information Governance Team, will instigate an investigation into the alleged unusual data activity of that member of staff and will report the results to the IAO and SIRO as appropriate.

- The Clinical Implementation Manager will ensure unusual data activity is entered as an incident if appropriate.

- If the unusual data activity cannot be appropriately investigated at Trust level, the Trust will contact the software owner to perform a full audit. The results of the report will be relayed to the appropriate Service Lead and investigator.

- Appropriate action will be taken against anyone found to have breached Trust policies and procedures relating to the use of a system, patient/staff confidentiality and data protection.

- The Clinical Implementation Manager will report to the Information Governance Sub-group on incidents as necessary.

If the audit results in being classified as a serious incident, the Incident Reporting Policy process must be followed. If it results in a Serious Incident (SI), the process will follow the Reporting Procedure for Serious Incidents (SIs) for Personal Identifiable Data

8 Consultation

Key individuals/groups involved in the development of the document to ensure it is fit for purpose once approved.

Name	**Designation**
Information Governance	Information Governance Sub Group
Anne Webb and Stephen Edwards	Library Services

9 Dissemination and Implementation

9.1 Dissemination

The Head of Information Governance will disseminate this policy to staff using the Trust Intranet site (the Hub) and bulletin.

9.2 Implementation

The Trust will ensure that appropriate processes are in place that detail how this policy will be implemented. The policy will be included in training sessions.

New employees will be made aware of this policy through the Induction process.

10 Process for Monitoring Compliance and Effectiveness

The implementation and compliance with this policy will be monitored by the Information Governance Sub-group.

Quarterly reports will be provided to the Information Governance Sub-group to monitor compliance.

11 Standards/Key Performance Indicators

IG Toolkit.

12 References

Data Protection Act 1998, c.29 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents

General Data Protection Regulation 2016/679/EU, *OJ L 119*, 4.4.2016, pp1-88 Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Information Governance Alliance (2016) Records management code of practice for health and social care 2016 [online]. Available at: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

Human Rights Act 1998, c.42 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/42/contents

ISO/IEC (2013) ISO/IEC 27001:2013 Information technology: security techniques: specification for an information security management system. Geneva, Switzerland: ISO/IEC.

Ministry of Justice (2013) Secretary of State’s Code of Practice (datasets) on the discharge of public authorities’ functions under Part 1 of the Freedom of Information Act: Issued under Section 45 of the Freedom of Information Act [online]. Available at: https://www.gov.uk/government/publications/secretary-of-states-code-of-practice-datasets-on-the-discharge-of-public-authorities-functions-under-part-1-of-the-freedom-of-information-act

Data Protection (Processing of Sensitive Personal Data) Order 2000, SI 2000/417 [online]. Available at: http://www.legislation.gov.uk/uksi/2000/417/contents/made

Senior Information Risk Officer Duties and Responsibilities

The Senior Information Risk Owner (SIRO) is an Executive Director of the Board who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk.

The SIRO is expected to understand how the strategic business goals of the Organisation and how other NHS Organisations' business goals may be impacted by information risks, and how those risks may be managed.

The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation.

The SIRO will be required to undertake information risk management training every three years to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

The SIRO is responsible for ensuring that all IAOs undertake training and resource in-house training on a three yearly basis.

- Key Relationships within the organisation
- Chief Executive and other Board members
- Caldicott Guardian
- Assistant Director of IT
- Head of Risk
- Head of Information Governance
- Information Asset Owners
- Information Security Lead
- Programme Managers, Technical Architects.

Regularly has contact with:

Chief Executives, Caldicott Guardians and Information Governance Leads of Department of Health and other NHS Organisations.

KEY RESPONSIBILITIES

Policy and process

- Oversee the development of an Information Risk Policy. This should include a Strategy for implementing the policy within the existing Information Governance Assurance Framework and be compliant with NHS IG policy, standards and methods.

- Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Annual Governance Statement.

- Ensure that the Board are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.

- Review and agree actions in respect of identified information risks.

- Ensure that Trusts' approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.

- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.

- Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities.

Incident Management

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation and that perceived or actual information incidents are managed in accordance with NHS IG requirements.

- To ensure that there are effective mechanisms in place for reporting and managing Serious Incidents (SIs) relating to the information of the Trust. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

Leadership

- Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.

- Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising.

Appendix 2

Information Asset Owner Duties and Responsibilities

The Information Asset Owners (IAO's) are senior members of staff who are the nominated owners for one or more identified information assets of the organisation. It is a core IG objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.

IAO's will work closely with other IAO's of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation. IAO's will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes
- How information is created, amended or added to over time
- Who has access to the information and why
- Audit the system for which they are responsible as se out in the Information
- Asset and System Audit Policy.

The IAO shall receive training as necessary to ensure they remain effective in their role as an Information Asset Owner.

Key Relationships

Within the Organisation:

- SIRO
- Caldicott Guardian (for assets that process patient data)
- Clinical Implementation Manager
- IG team
- Head of Risk
- Information Security Lead
- Other Information Asset Owners
- Information Asset Administrators
- Users of the Information Assets they own.

Key Responsibilities

Policy and Process

- Identify and document the scope and importance of all Information Assets they own. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the Information Asset.

- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks.

- Provide support to the organisation's SIRO and Risk Management Board to maintain their awareness of the risks to all Information Assets that are owned by the organisation and for the organisation's overall risk reporting requirements and procedures.

- Ensure that staff and relevant others are aware of and comply with expected IG working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.

- Provide a focal point for the resolution and/or discussion of risk issues and issues affecting their Information Assets.

Incident Management

Ensure that the organisation's requirements for information incident identification, reporting, management and response apply to the Information Assets they own. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.

Leadership

Foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the organisation's policy.

Training

The IAO will be required to undertake information risk management training every 3 years to demonstrate their skills and capabilities are up to date, and relevant to the needs of the Information assets they own.

Varied components of an Information Asset owned by the IAO. These include:

- Databases and data files
- System information and documentation
- Research information
- Operations and support procedures

- Audit data
- Manuals and training materials
- Contracts and agreements
- Business continuity plans
- Back-up and archive data
- Applications and System Software
- Data encryption utilities
- Development and Maintenance tools
- Computing hardware including PCs, Laptops, mobile communications devices e.g. blackberry and removable media
- Environmental services necessary for the safe operation of Information assets e.g. power and air-conditioning
- People skills and experience
- Shared services, including networks and printers
- Paper records, including patient case notes and staff records.

This above list is illustrative only and should be considered when identifying and recording an Information Asset, and for consideration of risks to that asset.

NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Appendix 3

Audit – unusual activity in units on SystmOne and stand-alone Electronic Patient Records Systems

Service:

Locality

Name of auditor

Contact details

Is this a re-audit? ☐ Yes ☐ No

If Yes, have previous audit actions have been implemented? ☐ Yes ☐ No

System being audited		
Unit/s being audited		
Time and date	Time	Date
Has any unusual activity been identified?	Yes	No
If yes, details		
Has an incident been raised on Ulysses	Yes	No
Ulysses number		
Date of next audit		

Completed audit to be retained in department and a copy sent to IG.BCHT@bridgewater.nhs.uk

If any unusual activity is found. Please complete the Clinical Systems Audit - Investigation form, which can be found here and contact the IG team.

Information Governance use:

Has a Clinical Systems Audit - Investigation form been completed

Name of the person investigating the unusual activity?

Date investigation commenced?

Date investigation ended?

Outcome of investigation?