Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title: Information Risk Management Policy

Version: 1.1

Reference Number: CO118

Keywords

Information Risk, Data Flow Mapping, Privacy Impact Assessment, Senior Information Risk Owner, SIRO, Information Asset, Information Asset Register, Information Risk Register

Supersedes

Supersedes: V1

Description of Amendment(s): Update to reflect the fact that the IG Manager has delegated IG incident management to the records manager (Section 13).

Originator

Originated By: Sarah Browne

Designation: Senior Information Governance and Risk Officer

Equality Impact Assessment (EIA) Process

Equality Relevance Assessment Undertaken by: Sarah Browne

ERA undertaken on: 15/11/2016

ERA approved by EIA Work group on: 14/12/2017

Reviewed as appropriate:

Where policy deemed relevant to equality-
EIA undertaken by N/A
EIA undertaken on N/A
EIA approved by EIA work group on N/A

Approval and Ratification **Referred for approval by: Sarah Browne** **Date of Referral: 17th November 2016** **Approved by: Information Governance Assurance Group** **Approval Date: 17th November 2016** **Date Ratified by Executive Directors : 16th January 2017** **Executive Director Lead: Executive Director of Finance**
Circulation **Issue Date: 20th March 2017** **Circulated by: Information Department** **Issued to: An e-copy of this policy is sent to all wards and departments** **Policy to be uploaded to the Trust's External Website? YES**
Review **Review Date: 16th January 2019** **Responsibility of: Sarah Browne** **Designation: Senior Information Governance and Risk Officer**
This policy is to be disseminated to all relevant staff. **This policy must be posted on the Intranet.** **Date Posted: 20th March 2017**

Information Risk Management Policy

Contents

1. Introduction

1.1 Our information is one of our most important assets. It allows us to identify our service users and their needs. It allows us to identify the suitability and availability of employees to coordinate our services. It allows us to pay for goods and services that are necessary to care for our service users. Without it, we cannot meet our core functions. As such, we have to take steps to protect our information from loss, inaccessibility, and unauthorised amendment or disclosure.

Each day, every staff member helps the Trust manage information risk by changing their passwords, reporting accidental disclosures as incidents, taking service users to quiet areas to have confidential conversations, and so on. This policy outlines the formal requirements of staff to manage information risk to ensure, as a Trust, we are handling information ethically, morally, and legally.

1.2 An Information Risk Management programme is required for compliance with the Information Governance Toolkit, and the national "NHS Information Risk Management" guidance published by NHS Digital. This requires each NHS organisation to identify an Accounting Officer (the Chief Executive), a Senior Information Risk Owner, and an information risk management structure (in the Trust's case, Information Asset Owners (IAOs), Information Asset Managers (IAMs), and Information Asset Administrators (IAAs)). Each information asset has an assigned IAO, IAM, and IAA.

1.3 Furthermore, the programme will evidence our compliance with principle 7 of the Data Protection Act (1998) that requires the Trust to take *appropriate technical and organisational measures […] against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.* The programme will allow us to identify vulnerabilities within our assets, identify threats that could exploit those vulnerabilities, the likelihood of such exploitation occurring, and the impact it would have on the asset, the information contained within it, and the organisation as a whole.

1.4 The programme will also allow us to evidence our compliance with:

- The S.46 Code of Practice under the Freedom of Information Act (2000), which requires identification and secure processing of records across the public authority
- Principles 1 and 2 of the Data Protection Act (1998) by recording the legal basis of our data flows
- Principles 3, 4 and 5 of the Data Protection Act by identifying where all information assets are held within the Trust. This will improve organisational memory and compliance with retention schedules as each IAO, IAM and IAA will have awareness of their asset remit.

- Principle 6 of the Data Protection Act (1998), as a record of all information assets will assist us in identifying individual patient records when required for the purposes of subject access or upon a request to prevent processing, for example.

1.5 This policy does not aim to eliminate information risk – as a whole – across the Trust. Rather, it will provide a programme that will allow the formal identification, prioritisation and management of information risks within the Trust.

1.6 While the Trust acknowledges that information risk is an essential element of information governance, the Trust considers the management of information as an integral part of good office management. The intent is to embed information risk into everyday practice to appreciate the practical benefits of understanding what information we hold, how it is received by the organisation, where it goes within and outside the organisation, and the legal basis for this. Identifying our information assets and flows of information will allow teams to benefit from reduced risk to their assets, work in a more efficient manner by decreasing the likelihood of records loss and system failures, and reduce the risk of information-related incidents within each team.

2. Purpose

2.1 The purpose of the Information Risk Management Programme (IRMP) is ultimately to manage information risk within the Trust at an acceptable level, consciously monitoring each risk.

2.2 The programme will support the Trust's corporate risk strategy, Information Governance Framework and the Information Governance, Records Management, Information Security and ICT suite of policy and procedures.

2.3 A number of key requirements in the relevant Information Governance toolkit form the basis of the IRMP, including:

- Identifying an Information Risk Management structure
- Mapping flows of information
- Identifying and maintaining a register of information assets
- Risk assessing information assets upon their implementation, periodically, after changes to the asset (or processes using the asset) and after incidents
- Setting out continuity plans for periods of information unavailability
- Management of records

3. Scope

3.1 This policy applies to all staff employed by the Trust, contractors, volunteers, agency, locum and bank staff and those providing a service on behalf of the Trust. The policy also captures all recorded information held by – or on behalf of – the Trust, including both paper and electronic records.

3.2 Compliance with Trust policies is a condition of employment, and breach of policy will be managed in accordance with the appropriate Trust Disciplinary Policy/Procedures.

3.3 The policy captures all types of risks to, and within, the Trust's information assets, and how they should be managed i.e. the management of threats to information assets, management of vulnerabilities within information assets, and management of possible impacts on information assets.

4. Related Documents

- Confidentiality Policy
- Corporate Risk Register
- Data Protection Policy
- Guidance for the retention of clinical and corporate records
- IG Requirements For New Processes And Systems (PIA)
- Incident Reporting, Management and Investigation Policy
- Information Governance Management Framework
- Information Governance Policy
- Information Governance Staff Handbook
- Information Governance Strategy
- Information Risk Assessment Standard Operating Procedure
- Information Risk Register
- Information Security Policy
- Information Sharing Policy
- Missing Records Procedure
- Network Security Policy
- Privacy Notice
- Training Needs Assessment
- Protocol For The Management Of Business & Corporate Records
- Protocol for the Management of Community Services Health Records
- Protocol for the Management of Mental Health & Specialist Services health records
- Records Management Moving Procedure
- Records Management Policy
- Risk Assessment Policy
- Risk Management/Risk Register Policy

- The Transition from Paper to Electronic Records and How to Volumise

5. Roles and Responsibilities

5.1 *The Chief Executive*

The Chief Executive, as Accounting Officer, has overall accountability for information governance within the Trust, and with the support of his Executive Directors, will ensure that the Trust complies with legislation and regulation affecting the handling of information. They will have responsibility for putting in places structures and processes. They will ensure information risks are assessed and mitigated to an acceptable level, and will report this as part of the annual *Statement of Controls.*

The Chief Executive delegates authority to the functions of SIRO, Caldicott Guardian and Information Governance Assurance Group (IGAG) (delegated responsibilities outlined below)

5.2 *Senior Information Risk Owner*

All NHS Trusts are required to have a Senior Information Risk Owner (SIRO) who is nominated by the Chief Executive, who will be a member of the Trust Board. The SIRO is accountable for information risk management within the Trust, and will ensure an appropriate information risk management framework is in place. The SIRO will foster a culture of protecting and using data, and will act as advocate for information asset management. The SIRO will represent matters pertaining to information risk on the board.

The SIRO will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18

Please see the Trust Information Governance policy for full list of the SIRO's key responsibilities.

5.3 *Caldicott Guardian*

The Caldicott Guardian has responsibility for ensuring that the principles of confidentiality are applied throughout the Trust, and for considering any applications to share information. The Caldicott Guardian will make representations regarding patient identifiable data within the IRMP.

The Caldicott Guardian will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.4 *Information Governance Manager*

The Information Governance Manager will assist the SIRO and Caldicott Guardian in ensuring the IRMP's compliance with national information risk

and confidentiality policy and legislation, and will oversee the operational management of the IRMP.

The Information Governance Manager will also record, assess, delegate for investigation and report on any incidents or breaches of policy or legislation via the appropriate channels, and in accordance with local and national incident reporting policy.

They will also ensure appropriate resources are available to the Information Governance team to enable compliance with this policy.

The Information Governance Manager will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.5 *Senior Information Governance and Risk Officer (SIGRO)*

The SIGRO shall have responsibility for implementing a robust information risk management programme throughout the Trust, ensuring compliance with legislation and national policy in relation to the management of information risk. The SIGRO will report progress of the IRMP to the Information Governance Assurance Group and Information Governance Managers Meeting, reporting back risk assessment findings.

The SIGRO will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.6 *Information Governance Assurance Group (IGAG)*

The Information Governance Assurance Group will oversee the IRMP. IGAG is the information governance steering group for the Trust, and consists of the Caldicott Guardian, the Senior Information Risk Owner, the Information Governance team, and Information Asset Owners/Managers/Administrators from all divisions across the Trust. The group will support and drive the IRMP through the organisation. Via the SIRO, IGAG will provide the Board with the assurance that an effective IRMP is in place within the organisation. This includes monitoring compliance with the IG Toolkit, and monitoring information risk work streams, the information asset register, and progress of the IRMP.

5.7 *Information Governance Managers Meeting*

The Information Governance Managers Meeting (IGMM) is held once a month to discuss current information governance projects and workflows, including information risk. Working under the authority of IGAG, members will collaborate to ensure appropriate information risk measures have been undertaken within the current workstreams (e.g. risk assessments or privacy impact assessments), and as a group will monitor trends in information risk incidents.

5.8 *Information Asset Owners (IAOs)*

The Trust's Information Asset Owners (IAOs) are Board-level/Director/VSM level members of staff who have overall accountability for the assets within the services under their remit. They will assist in identifying strategic threats and vulnerabilities, both internally and externally, to their services (and as such their information assets), and will advise on the impact such risks would have at a strategic level. They will have an understanding of the strategic value of each asset within their service, and – with the assistance of the IAM – will identify critical assets within their remit.

They shall also ensure that information risk assessments are reviewed each quarter on all information assets where they have been assigned 'ownership', following guidance from the SIGRO.

They will be responsible for nominating appropriate Information Asset Managers for each information asset.

IAOs will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

Please see the Trust Information Governance policy for full list of key IAO responsibilities.

5.9 *Information Asset Managers (IAMs)*

The Trust's Information Asset Managers (IAMs) are Service/Department Manager level staff and will coordinate the identification of information assets within their remit and will assign an Information Asset Administrator for each asset.

The IAM will have a thorough understanding of their information assets; their importance to the organisation, their links and dependencies on other assets, tactical threats and vulnerabilities facing the assets, and the direct and indirect impact these risks would have on the Trust.

They will ensure that:

- Risk assessments, Business Continuity Plans (BCP) and System Level Security Policies (SLSPs) are completed for each information asset
- Privacy Impact Assessments (PIAs) are conducted where required
- Data flows are mapped for each asset (see Appendix 1 for further information regarding documentation)
- The Information Asset Register is accurate and up to date.

The IAM will nominate an appropriate IAA for each information asset.

IAMs will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.10 *Information Asset Administrators (IAAs)*

The Trust's Information Asset Administrators (IAAs) can be any member of staff with an in-depth working knowledge of the asset and data flows, ideally Operational Manager (e.g. supervisor or team leader), but can be any officer, as appropriate. The IAA will have a thorough understanding of how the asset is used on a day-to-day basis, and how and when information is added and removed from the asset.

IAAs ensure that policies and procedures are followed regarding their asset. They will proactively and reactively recognise actual or potential security incidents, and will consult their IAO/IAM regarding incident management. They will assist in the identification of threats and vulnerabilities within the asset, documenting the flow of their assets, and in determining the value of their asset.

IAAs will work with IAMs to ensure risk assessments, SLSPs and PIAs are undertaken as appropriate (see Appendix 1 for further information regarding documentation).

IAAs will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.11 *Line Managers / Senior Managers*

All Line Managers must know the Information Asset Manager and Information Asset Owner for the assets they work with. They have responsibility for ensuring any information risk incidents are reported in accordance with the *Incident Reporting, Management & Investigation Policy* (see section 13 below). They will assist in the identification of assets, assessing asset value, mapping the flow of data in the asset, and identifying threats and vulnerabilities in each asset. They shall also ensure their staff, including volunteers, contractors, temporary, agency, locum or bank staff are vetted to an appropriate level, and – where consummate to their role – a confidentiality agreement is completed.

Line managers will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

5.12 *All employees and contractors, and anyone providing a service on behalf of the Trust.*

All employees and contractors of the Trust, and anyone providing a service on behalf of the Trust, whether permanent, temporary or contracted, have responsibilities for information risk on a day-to-day basis, whether they work in a clinical or non-clinical environment. They are responsible for ensuring that they are aware of the requirements incumbent upon them, and for ensuring that they comply with these. Any information governance incidents must be

reported to line management, and submitted via the Incident Reporting portal as per the *Incident Reporting, Management & Investigation Policy*.

Guided by their line manager, each staff member will undertake the required training tailored for their role in accordance with the Trust's IG Training Plan 2015-18.

6. Definitions

6.1 *Privacy Impact Assessment (PIA)*

"A process which assists organisations in identifying and minimising the privacy risks of new projects or policies" – Conducting Privacy Impact Assessments: Code of Practice, The Information Commissioner's Office.

A PIA helps an organisation to identify and reduce the privacy risks of a new process, service, information system, or information asset. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes.

It enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

For more information about your responsibilities regarding PIAs, please see Appendix 1 and the *"Information Governance Requirements for New Processes, Services, Information Systems and Assets"* policy.

6.2 *Data Flow Mapping*

This is the process of documenting the transfer, or "flow", of information from one physical location to another, recording the method by which it "flows", and the legal basis that allows the "flow". Types of data flows may include: email, fax, post/courier, text or transfer to portable electronic/removable media. Appendix 1 outlines when data flow mapping should occur, and be reviewed.

6.3 *Threat (also see Hazard)*

"A potential cause of an unwanted incident, which may result in harm to a system or organisation" – ISO/IEC 27000:2014

There are seven main categories of threats/hazards:

- Malware – e.g. Computer virus
- Physical – e.g. Theft of laptop
- Misuse and/or abuse – Unauthorised access to electronic patient record
- Social engineering – e.g. Person pretending to be patient's relative to obtain patient information
- Hacking – e.g. Hacking into the system to modify data

- Environmental – e.g. vandalism, fire, flooding
- Errors and/or failures – e.g. Computer crashing as system, overloads

6.4 *Hazard (also see Threat)*

"A source of potential harm" – ISO Guide 73:2009

Hazards are generally viewed as a natural source of threat e.g. flooding, fire, earthquakes. Both threats and hazards should be considered in assessing risk.

6.5 *Vulnerability*

"The intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence" – ISO Guide 73:2009

Vulnerabilities are weaknesses within or surrounding our information assets that leave them susceptible to an attack from a threat.

Vulnerabilities may be *intrinsic* (something inherent to the asset), or *extrinsic* (the way the asset is utilised, modified, or processed).

6.6 *Impact*

The outcome of an event on the Trust's objectives and service delivery.

6.7 *Risk*

Risk is the sum of impact (or consequence) and the likelihood of that impact occurring. Threats may attack vulnerabilities within the asset, increasing the likelihood of that consequence occurring. This creates risk.

6.8 *Information Asset*

Assets that are of value to the organisation (e.g. necessary for service delivery or corporate function) that contain information. The information contained within the assets could be patient identifiable data, or it could be corporate information.

This will include all assets that are necessary for the effective running of the Trust (e.g. patient information, finance information, stock controls etc.) and the software, computer systems, and network infrastructure that are used to process such data.

Paper records holding information will also constitute information assets, whether on or off site.

There are six main categories of information asset:

- Information – e.g. contained within databases, system documents, policies, procedures, and archived files
- Software – e.g. application programs, systems, ICT development tools and utilities
- Physical – e.g. infrastructure, equipment, furniture and accommodation utilised to allow the processing of data
- Services – e.g. including ICT for computing and communications, or Estates for heating, lighting and power that are utilised to allow the processing of data
- People – e.g. their qualifications, skills and experience that are utilised in the processing of data
- Non-Tangible Assets – e.g. Trust reputation, goodwill of service users, suppliers, partners, potential partners and employees

6.9 *Information Asset Register (IAR)*

The information asset register is a repository of information assets held by the Trust. It has been formulated from previous information asset tool returns, and is managed by the Information Governance team. Each quarter the Information Asset Owner (with the assistance of their Information Asset Managers and Administrators) will review their entries on the IAR, and advise the Information Governance team of any changes (e.g. new assets, changes to the assets, termination of any assets etc.).

6.10 *Risk Assessment*

The overall process of risk identification, risk analysis and risk evaluation.

6.11 *Risk Matrix*

A table that allows us to score risk based on the likelihood of an event occurring multiplied by the impact the event would have.

6.12 *Risk Evaluation*

The process of scoring the risk found within the risk analysis.

6.13 *Control*

A measure that is put in place to modify (most likely, reduce) risk.

6.14 *Risk Treatment*

The process of modifying risks by putting controls in place. There are four main types of risk treatment:

1. Avoid the risk – terminate the source of the risk
2. Share/transfer the risk to a third party– e.g. Obtain insurance against theft
3. Reduce the risk – By putting controls in place
4. Accept the risk – After the risk has been accepted it should be regularly monitored for any changes

6.15 *Residual Risk*

The risks remaining after risk treatment (including accepted risks).

7. Risk Assessment Toolbox

7.1 The Information Governance team has developed tools to record the identification of information assets and data flows. The IAO will ensure both tools are completed for each asset within their remit.

7.2 The team has also developed a risk assessment tool that should be used to record information risks for each asset. Risk assessment should be conducted in accordance with the *Information Risk Assessment Standard Operating Procedure* and reviewed in accordance with Section 12 – Monitoring and Review.

7.3 The result of each risk assessment will be recorded locally in Information Governance. Where risks are found to be "high" they will be added to both the Corporate Risk Register and the Information Governance Risk Register, and will be monitored in line with the Trust's *"Risk Management/Risk Register policy"* and the "*Information Risk Assessment Standard Operating Procedure".* Where risks are found to be "moderate" they will be added to the Information Governance Risk Register, and will be monitored in line with *"Information Risk Assessment Standard Operating Procedure."*

8. Risk Scoring

8.1 The IAM will be responsible for ensuring risk assessments are undertaken on each asset within their remit. Information Governance team will then assist in scoring the risk assessment once it has been completed.

8.2 Once risk analysis is undertaken, a risk score will be obtained which will denote risks as "high", "moderate", "low risk" and "very low risk". The "*Information Risk Assessment Standard Operating Procedure"* will outline how risks are score, and the actions that should be taken regarding each level of risk.

9. Risk Treatment Budget

9.1 If risk treatment will incur a financial cost, the IAO will be responsible for making financial arrangements to fund the treatment.

9.2 All risk treatment decisions will be reported to the SIRO.

10. Training

10.1 The SIGRO will provide IAOs, IAMs, and IAAs with face-to-face training to ensure they understand their role. The contents of this policy, asset identification, and threat and vulnerability identification will be covered.

10.2 All staff will undertake training online in accordance with the Trust's IG Training Plan 2015-18 which is available on the intranet or via the Information Governance team.

11. Communication and Consultation

11.1 IGAG will be the central arena for:

- Reporting on the development of the IRMP
- Reporting on results of data flow mapping, risk assessments, and reporting actions that have been taken to treat risks

11.2 IGMM will be the arena for:

- Monitoring individual workflows pertaining to information risk
- Collaboration regarding the advancement of the IRMP through the Trust
- Feedback from information governance subject matter experts regarding the outputs from the data flow mapping, information asset identification, privacy impact assessment and risk assessment exercises

11.3 The SIRO will receive quarterly reports regarding:

- All risk treatment decisions made – via IGAG
- All risk assessments scoring "moderate" (amber) or "high" (red) (i.e. 8 or above) and subsequent risk treatment decisions
- The Information Asset Register
- The Information Risk Register

12. Monitoring and review

12.1 Every quarter, the IAO – with the assistance of their IAMs and IAAs where necessary – will review their completed risk assessments. They will consider whether any new risks have arisen, and if there has been a change in:

- Risk appetite
- Likelihood
- Impact

12.2 Where there is a change in the use of the asset, or an incident occurs involving the asset, the completed risk assessment will again be reviewed to consider whether there has been a change in risk appetite, and to check accuracy of the recorded:

- Threats
- Vulnerabilities
- Likelihood
- Impact

12.3 The result of this review will be fed back to the SIGRO who will record the review locally, update the review on appropriate risk registers (as required), and feed back to IGMM.

12.4 The IRMP policy will be reviewed annually, or as required by new national requirements or legislation.

13. Incident Reporting

13.1 Any incident that results in harm to the confidentiality, integrity or availability of Trust information constitutes an information risk incident.

13.2 All information risk incidents should be reported in line with the *Incident Reporting, Management & Investigation Policy* via the Safeguard/Incident reporting portal on the Intranet.

13.3 The Risk Department will notify the Information Governance Manager of any information risk incidents. Where required, the Information Governance Manager may delegate any of the below responsibilities to an appropriate member of staff for completion. Responsibility for the below is currently delegated to the Trust's Records Manager.

13.4 Where an investigation is required, the Information Governance Manager, or delegate, will decide who should lead the investigation; the service, or information governance.

13.5 The Information Governance Manager, or delegate, will consider all information risk incidents against the *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation* published by NHS Digital. If the outcome – in terms of the severity of the incident – is IG SIRI level 2 (reportable) this will be reported via the on-line Information Governance Toolkit (IGT) incident reporting tool resulting in an email notification being sent to the NHS Digital External IG Delivery Team, Department of Health, and ICO and escalated to other regulators, as appropriate. IG SIRI level 1 or less outcomes will not be reported via the IGT incident reporting tool and, therefore, no notifications will be sent.

13.6 After an incident or near-miss, the asset should be reviewed in line with Appendix 1.

14. Recovery and Contingency

14.1 All information assets will have an associated business continuity plan (BCP). Where the asset is an ICT system, one copy shall be held with ICT, and the IAO, IAM and IAA shall have a copy. For paper assets, a copy should be held by the IAO, the IAM and the IAA.

14.2 When recovery or contingency issues arise, the IAO for that asset is responsible for the implementation if the BCP.

Appendix 1 Information Risk Management Documentation Process