NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Information Asset and System Management Policy

Policy Number	**IG/Pol/005**
Target Audience	**Information Asset Owners, Information Asset Administrators, Budget Holders who procure information assets and systems, Programme and Project Managers**
Lead Executive Director	**Director of Finance/Senior Information Risk Owner**
Recommending Committee/Group	**Digital Information Governance and Information Technology**
Approving Committee(s)	**Corporate Clinical Policy Group**
Ratifying Board	**Trust Board**
Date First Ratified	**February 2012**
Last Full Review Date	**December 2021**
Next Full Review Date	**December 2023**
Lead Author(s)	**Information Governance and Records Manager**
Version Number	**4.0**

Applicable Statutory, Legal or National Best Practice Requirements	UK GDPR 2018 and Data Protection Act 2018 Department of Health and Social Care (2021) NHS Digital (2013, updated 2016, 2018) DCB0129 NHS Digital (2013, updated 2016, 2018) DCB0160 NHS Digital (2021) Clinical risk management standards

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
1.0	Feb 12	IG Subgroup	Policy Approval Group
2.0	April 2016 April 2016 April 2016 April 2016	Head of IG Policy Approval Group J. McCartney D. Williams	Minor updates to roles and terminology Approved subject to minor amendments to S. 1, 3, 6, 7.1, 8 & 9 Amendments completed; references updated Final chair approval
3.0	January 2018 April 2018 April 2018 April 2018	IG Subgroup Policy Approval Group J. McCartney S. Arkwright	Minor updates, name changes Approved subject to minor amendments Amendments completed Approved by chair action
3.1	July 2021	Sharon Ramsdale	Full review, supersedes previous policy.
3.2	October 21	Mary Corkery	Comments made
3.3	November 21	Digital Information Governance and Information Technology	Signed-off
3.4	November 21	Mary Corkery	Comments made
3.5	December 21	Corporate Clinical Policy Group	Approved, submitted for ratification by the Trust Board
4.0	3rd February 2022	Trust Board (e-governance)	Ratified – Policy Officer notified 28/02/2022

Equality Impact Assessment	Required?	Action Required
Does this policy impact/potentially impact on: • **Staff** • **Patients** • **Family Members** • **Carers** • **Communities**	**Yes** →	**Contact the Trust's Equality & Inclusion Manager at:** **Email: ruth.besford@nhs.net** **Date contacted:**
	No →	**Complete details below:** **Name: Sharon Ramsdale** **Email: Sharon.Ramsdale@nhs.net** **Date: 30.11.21**

Education & Professional Development Question

To ensure training requirements are discussed and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements.

Please answer the following question by entering a cross in the Yes or No box below:

	Yes	No
Does this document have any additional training requirements or implications?		x

If you have answered **YES** you must forward a copy of this document to Education & Professional Development **before** submitting to the Policy Officer or HR Project Officer.

Date submitted to Educations & Professional Development: ……

No further action is required if you have answered NO.

Contents

1 Introduction

This document outlines the responsibilities and the process in which Bridgewater Community Healthcare NHS Foundation Trusts (hereafter the Trust) Information Assets (IA) including Information Systems are maintained and managed. The Trust Information Assets and Information Systems are to be managed in accordance with NHS digital, Information Governance (IG), Information Technology (IT), Information Security and Record Management (including clinical systems) and Procurement policies.

Each information asset within the Trust has/will have an Information Asset Owner (IAO) assigned at Executive or Senior Management level, this person is responsible for ensuring the integrity, security, function, and management including any associated Agreements, including third party contracts.

NB: It is expected that all IA placed on the Information Asset Register have been through the Trusts due diligence process which includes a Data Protection Impact Assessment (DPIA), an appropriate agreement and/or contract in place; any health/clinical systems have Clinical Safety standards, DCB0129 and DCB0160.

This will ensure the Trusts Data Controller responsibilities can be evidenced and monitored within an agreement and/or contract. All IA procured from Third Parties need to have a written contract with the appropriate Data Processors clauses embedded, to meet legal requirements - see the Information Governance Framework and the Data Protection and Confidently Policy for more details.

The role of IAO was created following the UK Government's 2008 review of data handling within Government against the backdrop of high profile data losses. The review focussed initially on personal data handling but also covered any sensitive information processed by an organisation.

The recommendations of the review stressed the need to manage Information Assets in compliance with various statutory obligations it suggested that three new roles be established to facilitate the management of information: Senior Information Risk Owner (SIRO), IAO and Information Asset Administrator (IAA).

The IAO role now forms an integral part of the Data Security and Protection Toolkit (DSPT) which is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

1.1 Objective

To ensure all Information Assets and associated information systems are managed within a legal framework

To ensure the security and protection and therefore the confidentiality, integrity and availability of the Trust's data. To this end the system/IAA managers should:

- Ensure availability of data when required by users
- Preserve confidentiality
- Protect assets against unauthorised disclosure
- To ensure all audits are undertaken on the information asset are done within a standard format.

1.2 Scope

This guideline is applicable to all Trust IAO's, IAA'S, Budget Holders who procure information assets and systems, Programme and Project Managers

2 Definitions

The definitions applicable to this document are as follows:

DPIA (Data Protection Impact Assessment)	A DPIA is a process to help you identify and minimise the data protection risks of a project. A DPIA must include: • Describe the nature, scope, context and purposes of the processing • Assess necessity, proportionality and compliance measures • Identify and assess risks to individuals; and • Identify any additional measures to mitigate those risks (Information Commissioner's Office (ICO, 2021)
Record of Processing Activities (ROPA)	The record of processing activities allows you to make an inventory of the data processing and to have an overview of what you are doing with the concerned personal data. The recording obligation is stated by Article 30 of the UK General Data Protection Regulation (GDPR).
Business Continuity Plan	A business continuity plan is a collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of a serious incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.

Disaster Recovery Plan	A disaster recovery plan is a documented process or set of procedures to protect and recover business IT infrastructure and systems in the event of a disaster. It describes the steps necessary to recover the system to a working state; the acceptable amount of data loss to the business; and how long the recovery is expected to take.
Active Directory	User access to Information Assets on the Trusts network is controlled mainly by NHS Active Directory. This is role based. For example, logging into a system using your personal computer (PC) log in or NHS.net address, is the Trusts active directory Therefore if you join or leave the Trust this is managed through the active directory.
Third party Access	Third party access to Information Assets will be based on a formal contract that satisfies all necessary NHS security conditions. Third party suppliers to the Trust and non-Trust devices are not allowed access to the Trust network unless authorised. Where data is shared with third party suppliers, an information sharing agreement must be in place before accounts are created.
System Level Security	System Managers in completing of a System Level Security assessment for each Information Asset. It is the IAA responsibility to complete and regularly review and identify changes to system use and to complete appropriate risk assessments.
Processing (of information)	Art.4(2) "Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Decommissioning	Decommissioning is a strategic approach for systematically ending a contract with a data processor who has access to our personal and sensitive information or retiring applications and costly outdated legacy applications without compromising business needs or compliance requirements.

Role based access	A process where depending on the Users role they will get access to different parts of the system. Privileged users or systems administrators have higher access to the system therefore by default have access to personal or special category information.
Information Asset	A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and used effectively. Any collection of personal data required to conduct an organisation's business and the technical equipment to manage this data are referred to as Information Assets. The term Information Asset is very wide ranging in what it can include any information that is processed, or linked to the IA in an Information System will typically contains the following components: • Hardware (linked to IA): computer-based information systems use computer hardware, such as processors, monitors, keyboard and printers i.e., collecting information (the asset cannot function if the information is not collected) • Software: these are the programs used to organise process and analyse data, e.g., databases, that collect, record and store information • Applications such as Attend Anywhere, Teams.
System Administrator	"Typically, responsible for installing, configuring and maintaining hardware and software infrastructure. Systems administrators by nature of their role have elevated rights compared to a normal user." (NHS Digital – Data Security Standard 4)
Senior Information Risk Owner (SIRO)	The SIRO will be an Executive Director or Senior Management Board Member 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
Information Asset Owner (IAO)	The responsibilities of an IAO is to manage the risks to personal information and business critical information held within a department and ensuring contracts or agreements are managed.

Information Asset Administrator (IAA)	An Information Asset Administrator (IAA) may be responsible for the day-to-day management of data. Granting and revoking access to confidential information. Recognising potential or actual security incidents. Consulting the IAO on incident management.

3 Abbreviations

The abbreviations applicable to this document are as follows:

IT	Information Technology
ESR	Electronic Staff Record
SIRO	Senior Information Risk Owner
IAO	Information Asset Owner
GDPR	General Data Protection Regulation
IA	Information Assets
IG	Information Governance
DPIA	Data Protection Impact Assessment
IAA	Information Asset Administrator
PC	Personal Computer
DPO	Data Protection Officer
ROPA	Records of Processing
PPDR	Performance and Personal Development Review
PID	Personal Identification Data
TOR	Terms of Reference
CNIO	Clinical Informatics Chief Nurse
ICO	Information Commissioner's Office
RM	Records Management
DIGIT	Digital Information Governance and Information Technology

4 Other Relevant Documents

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

Procurement Policy

Data Protection and Confidential Policy

Information Governance Framework Policy

Information Security Policy

Access Control Policy (Passwords etc)

Record Management: Archiving, Retention and Disposal Policy

Records Management: Storing and Movement of Records Policy

Corporate Records (including Document Management) Policy

Performance and Personal Development Review Policy

Risk Management Framework

Incident Reporting Policy

Mandatory Training and Induction Policy

Disciplinary Policy and Procedure

Anti-Fraud, Bribery and Corruption Policy

5 Roles and Responsibilities

5.1 Senior Information Risk Owner

The SIRO is the Board Member who has overall responsibility for Information Risk Management in the Trust. The responsibilities of the SIRO are to:

- Take overall ownership of the organisation's Information Risks
- Receive written assurance from IAO's on the required standards within this policy
- Understand how the strategic business goals and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the IG Risk Assessment and Management processes regarding procurement.

- Sign off and take accountability for risk-based decisions and reviews in regard to the processing of personal data within the Trusts registered Information Assets

- Advise the Board on the effectiveness of information risk management across the Trust.

The SIRO will report to the Quality and Safety Committee on information risks and through the Statement of Internal Controls following assurance from the Information Asset Owners.

The SIRO is the Director of Finance. The Deputy SIRO is the Assistant Director for IT.

5.2 Caldicott Guardian

The Caldicott Guardian is the Chief Nurse and is responsible for:

- Ensuring the Trust satisfies the highest practical standards for handling patient identifiable information

- Facilitating and enabling appropriate information sharing and make decisions on behalf of the Trust following advice on options for lawful and ethical processing of information, in particular in relation to disclosures

- Representing and championing IG requirements and issues at Board level

- Ensuring confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff

- Overseeing all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

The Deputy Caldicott Guardian is the Deputy Chief Nurse.

5.3 Assistant Director of IT

The Assistant Director of IT, supported by the Head of IT, the Chief Nursing Informatics Officer and the Head of Information and their teams is responsible for:

- Developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the Trust systems and infrastructure remain compliant with data protection legislation

- Ensuring appropriate usage, accuracy and that reasonable steps are taken to ensure personal data is accurate, having regard to the purposes for which they are processed, are erased, or rectified without delay implement best practices for data quality

- Ensuring all the Trust electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations

- Any health IT systems on the Trust domain that are used by care professionals is safe and that the organisations has met requirements stated in the two Clinical Safety standards, DCB0129 and DCB0160. These standards are mandatory under the Health and Social Care act 2012, ultimately, this helps health and care staff to provide better, safer patient care.

5.4 Information Asset Owner

The Information Asset Owner (IAO) is assigned at Executive or Senior Management level; this person is responsible for ensuring the integrity, security, function, and management including any associated contracts and or agreements. Their main responsibilities include:

- Providing assurance to the SIRO on the security and use of these assets on a yearly basis

- Continuing to maintain an understanding of 'owned' assets and how they are used for

- Approving information transfers and giving assurance to the SIRO that these transfers are secure

- Approving and overseeing the decommissioning of the asset (i.e., when the system provider moves from one provider to another)

- Managing the disposal mechanisms for information following the required retention is undertaken to legal standards

- Ensuring any health Information systems not managed by the Trusts IT Team are used by care professionals is safe and that the organisations has met requirements stated in the two Clinical Safety standards, DCB0129 and DCB0160. These standards are mandatory under the Health and Social Care act 2012, ultimately, this helps health and care staff to provide better, safer patient care

- The appropriate usage, accuracy and that reasonable steps are taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased, or rectified without delay implement best practices for data quality

- Knowing what information is held and who has access to it for what purpose

- Taking visible steps to ensure compliance with the Trust's IG Policies and policies

- Understanding any risks associated with the information asset

- Understanding and addressing the risks to the information asset and provides assurance to the SIRO

- Receiving logs and controls requests from other staff for access to the information asset or assign an appropriate person to act on my behalf

- Ensuring clinical systems meet clinical safety standards

- Ensuring an appropriate person is trained in monitoring clinical system standards and provided relevant support and advice to staff members

- Ensuring changes to the information asset are documented with a formal sign off from the IG department following the undertaking of a DPIA where necessary

- Ensuring risks relating to the IA is managed and mitigated in line with Trust policy

- Leading and fostering a culture that values, protects and uses information for the benefit of patients

- Appointing an appropriate IAA. NB: if an IAA is not appointed it is expected that the IAA will undertake all responsibilities

- Effective management and security of the Trust's Assets including IT resources, for example, infrastructure and equipment

- Developing and implementing a robust IT Disaster Recovery Plan, which is tested annually

- Ensuring IT security levels required by the NHS are met

- Ensuring the maintenance of all firewalls and secure access servers are in place at all times

- Acting as the Information Asset Owner with specific accountability services that are operated by corporate and clinical work force, e.g., personal computers, laptops, personal digital assistants and related computing devices, held as an Information asset

- Working with the IG team and Data Protection Officer (DPO) as appropriate regarding matters relating to data and IT security.

5.5 Information Asset Administrator/s (IAA)

The IAA is to be trained and have working knowledge of the system, their responsibilities include (more details can be found in section 7):

- Ensuring Trust policies including IG, Information Security policies and procedures are followed

- Ensuring any records of processing (ROPA) in relating to the Information Asset and is supplied to the IG team when requested

- Recognising potential or actual security incidents and escalate
- Consulting with the IAO on any incidents and undertake incident management responsibilities
- Ensuring compliance with data sharing agreements
- Ensuring information handling procedures are fit for purpose and properly applied
- Ensuring personal information is not lawfully exploited
- Undertaking a DPIA and manage associated risks and issues where highlighted
- Recognising new information handling requirements and ensure appropriate procedures are produced and embedded
- Recognising potential or actual security incidents and report as per Trust policies
- Reporting to on the current state of the information asset
- Ensuring the standards in this guideline are adhered and monitored
- Acting as a first port of call for local managers and staff seeking advice on the handling of information
- Ensuring any users of the IA is fully trained and understands the requirements of the system
- Ensuring the IA is only accessed by those who are authorised to do so
- Ensuring access to the IA is always secure and audited and any inappropriate access of the IA is reported via the Trust reporting system
- Ensuring an appropriate procedure/processes are in place to ensure information is managed, accessed and securely destroyed when there is no further requirement for it as per Trust Policy.

5.6 Data Protection Officer

The DPO for the Trust is held by the Trust Secretary. The DPO is responsible for reporting directly to the Board about data protection matters. These may include IG risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

The Information Governance and Records Manager is accountable to the DPO.

5.7 Information Governance and Records Manager

With the support of the IG team, the Information Governance and Records Manager is responsible for:

- Ensuring the Information Asset Register is maintained and updated under the direction of the IAO and the IAA
- Maintaining an awareness of information governance issues within the Trust
- Keeping up to date with changes in legislation to ensure the Trust remains compliant
- Reviewing and updating the Information Governance Framework Policy in line with local and national requirements
- Working with IAO, IAA and project managers to complete a DPIA and recommend any areas of risk
- Liaising with wider teams, like IT, Procurement, Information Security and Clinical Safety to support the IAO, IAA and project managers regarding management of the IA
- Reviewing and auditing all procedures relating to this policy where appropriate
- Ensuring line managers are aware of the requirements of the policy.

5.8 Staff with elevated access/privileged users

Staff with elevated access to IT/Information systems, including clinical systems and health records will be held accountable to the highest standards of use; they will be subject to higher monitoring and will have subsequent enhanced contract agreements – see section 7.7.

6 Equipment

Not applicable

7 Information Asset

7.1 Central Register

All Information Assets are registered by the IG Team and must be registered on the Trusts IA register and held centrally by the IG Team to maintain corporate oversight and to enable ease of reporting to SIRO and external regulators.

All information assets identified on the register must be classified based on the critical need of the organisation (see appendix two).

Each IAO should develop their business continuity plan based on the IA classification – see section 7.2.

Note: Some information assets are more critical than others.

7.2 Continuity Plan

All IA's must have an up to date and a yearly tested business continuity plan which includes a disaster recovery or a separate document to test the function of the plan and identify any areas for improvement.

7.3 Assessing and Classification

All information within the IA must be assessed and categorised by IAO/IAA with the appropriate marking to ascertain the types of information the asset holds and how to manage it.

- **Official:** Most organisations operate almost exclusively at this level. It is expected that normal security measures will be enforced through local processes and therefore provide sufficient levels of protection to information i.e., staff should be sufficiently aware and understand that they have a responsibility for securely handling any information that is entrusted to them.

- **Official-Sensitive: Personal** Information marked with this classification will be sensitive information relating to an identifiable individual (or group), where inappropriate access could have damaging consequences.

- **Official-Sensitive: Commercial** Information marked with this classification will be commercial or market sensitive information that could have damaging consequences including reputational damage if it were lost, stolen, or inappropriately published.

The classification above has been extracted from the Corporate Records (including document management) Policy, there are some examples in this policy, to help with the categorising of the data.

Note: if the IA contains multiple categorised, the highest category is to be used. For example: Electronic Staff Record (ESR) could potentially contain all of the above, therefore **Official-Sensitive: Personal** would be applied.

7.4 User Process

All IA's must have:

- A user process that assigns different levels of access, i.e., role based access, to ensure information is only accessed by those who need to access it

- A process that adds and removes authorised users, this includes levels of authorised access to ensure access rights are removed immediately and to give access to those in a timely manner.

7.4.1 Monitoring

All IA must have a process that monitors users access to ensure no authorised access by users. This can be undertaken by the IAA, or a team assigned. If inappropriate access is discovered, the incident managed process is to be followed.

7.4.2 Training

All IA must have a training schedule based on the level of access of the user to ensure users know their responsibilities and are able to do their job efficiently.

7.4.3 Privileged Access

All users must understand their access and those with privileged access are to have this reiterated at each Performance and Personal Development Review (PPDR), or those set by the IAO.

A suggested template to support this can be found in Appendix 1 – also see 5.3 in responsibilities

7.5 Data Flows

Information that is transferred in and out of the IA must be recorded, retained and audited yearly to ensure information has been legally shared. All transfers forms (bulk data transfers) are held with the IG team.

7.6 Third Party Transfers

It is a legal requirement that an agreement and/or contract must be in place prior to sharing information with a third party/outside the Trust.

Any third party transfers (information in and out) must be authorised by the IAO or equivalent (Caldicott guardian or SIRO), as per the Data Protection and Confidentiality Policy.

7.7 Quality of information

The quality of the information contained in the asset must be audited and reviewed on a scheduled programme of improvement, as per the Data Protection and Confidentiality Policy.

Where third party access is required, this must be registered and scheduled in line with IT services can schedule and support the third party access.

7.8 Password complexity meeting cyber security standards

Where an IA is accessed through the user access directory set by the Trusts IT Team, this must comply with cyber security standards. Where a IA/system is not managed in this way, it must have a password procedure based on the information contained in the Access Control Policy; this is a DPST requirement.

The IA must use access security settings approved by the Trusts Information Security Team to ensure there are no security issues identified.

Any IA that sends or receives information via electronic transfer must ensure it is encrypted/secure. All paper flows of information containing Personal Identification Data (PID) must be tracked and secure as per Record Management (RM) standards.

7.9 Risks

Any risks associated with the IA must be registered on the Trust corporate risk register.

All incidents reported on the IA must be reported on the Trusts Risk Management Reporting System (Ulysses) and managed as per the Incident Reporting Policy.

7.10 Retention and Disposal

To comply with legal requirement, the IA must have a retention and disposal process in line with the Trust Records Management: Archiving, Retention and Disposal Policy.

8 Consultation

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

Name	Designation
Jackie McKay	Senior Information Governance Officer
Mary Corkery	Policy Officer
DIGIT Members as per Terms of Reference (TOR)	Associate Director: Quality Governance Director of Finance/ Senior Information Risk Owner Responsible Assistant Director For IT/Deputy SIRO Information & Clinical Performance manager Data Protection Officer Head of IT Head of Data Security Clinical Informatics Chief Nurse (CNIO) Registration Authority & Training Lead Head of Procurement Director of Operations / Nominated Deputy – Warrington Director of Operations / Nominated Deputy – Halton & St Helens Director of Operations / Nominated Deputy – Dental Director of Operations / Nominated Deputy – Health and Justice Education & Professional Development Lead Human Resources

Name	Designation
Information Asset Owners	Distributed to registered IAO
Information Asset Administrators	Distributed to registered IAA
Razia Nazir	Knowledge and Library Services Manager
Corporate Clinical Policy Group	
Trust Board	

9 Dissemination and Implementation

9.1 Dissemination

This policy will be disseminated by the IG Records Manager to all registered IAO and IAA members of the DIGIT, DSPT Steering Group and Digital Programme Group.

The policy will be made available on the Trust intranet and internet and published in the team brief.

9.2 Implementation

This policy will be implemented through the DSPT and the audit programme.

10 Process for Monitoring Compliance and Effectiveness

Minimum Requirement	Frequency	Evidence	Response Committee(s)
DS&P Toolkit Annual Assessment	Annually for sign-off	Assessment of information submitted	DSPT Steering Group/DIGIT
Incident Analysis	Monthly/ Quarterly	IG report to DIGIT	DSPT Steering Group/DIGIT

11 Standards/Key Performance Indicators

Audit programme based on the standards set in this policy.

Note: The audit tools associated with this policy will be held with the Information Governance Team, as the tools will be piloted and enhanced based on action plans.

12 References

Data Protection Act 2018 c. 12 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents

Department of Health and Social Care (2016) Records Management: code of practice for health and social care [online]. Available at: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Health and Social Care Act 2012 c. 7 [online]. Available at: https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

Information Commissioner's Office (ICO) (nd) Data protection impact assessments [online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ Accessed on 30/11/21

Information Commissioner's Office (ICO) What do we need to document under Article 30 of the UK GDPR? [website]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/what-do-we-need-to-document-under-article-30-of-the-gdpr/

NHS Digital (2013, updated 2016, 2018) DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems

NHS Digital (2013, updated 2016, 2018) DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems

NHS Digital (2021) Clinical risk management standards [online] Available at: https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards Accessed 28/10/21]

Appendix 1

Privilege Users Example

Consider using this form as evidence of ensuring those with elevated access, know their obligations. It is recommended it is used when undertaking their annual PPDR.

Name	
Date of PPDR	

As a System administrator and/or a user with privileged access you have elevated rights compared to a normal user. This includes access to sensitive information which you would not normally be required to see as part of your role.

All systems within the trust, containing sensitive information are periodically reviewed and monitored to confirm no unauthorised access is being made.

To protect the integrity of all data in ensuring that information is only ever accessed, as the need arises, in your role as system administrator you are asked to confirm the following statements:

- All actions undertaken whilst working with sensitive data are taken with highest level of integrity in terms of respect of the confidentiality, integrity or availability of the systems I support.
- As system administrator I understand the responsibility in that all work should be undertaken in the knowledge of the appropriate system access policies and compliance with Information Governance standards.
- I understand that as a system administrator if I use data illegally/for my own gain, I could face disciplinary action which may lead to prosecution.

Manager's name	
System users signature (digital signature can be used)	

IA Classification

IA Classification (based on service provision)	Service Characteristics/provision
Platinum	• Typically, critical national services. • Absence of system leads to complete failure of dependent systems and services with a high possibility of clinical safety issues. • Service interruption results in severe reputational damage. • 24x7x365 Support required. • Service Availability – 99.9%. • DR Recovery target 2 hours. • Monthly MI reporting. • Example service – Spine.
Gold	• Predominantly transactional services. • Absence of system leads to operational difficulties that can be coped with for a limited period. • Absence of system may lead to increased risk to clinical care. • 8-6 Mon to Sat Support required. • Service Availability – 99.9%. • DR Recovery Target 4 hours. • Monthly MI reporting. • Example service – POS/DSCRO
Silver	• Predominantly data capture, batch processing. • Absence of system leads to operational difficulties, but these are manageable for an extended period. E.g., 1 day. • Absence of system may lead to a slight increase in clinical risk Business Hours Support (8am-6pm) Mon-Fri (not BH). • Service Availability – 99.5%. • DR Recovery optional - dependent on outcome of business impact analysis. • Monthly MI reporting. • Existing service – SUS, HES.
Bronze	• Business Hours Support (8am-6pm) Mon-Fri (not BH). • Service Availability – 98%. • DR Recovery optional- dependent on outcome of business impact analysis. • Ad Hoc MI reporting. • Existing service – Parliamentary questions/publications.