University Hospitals of North Midlands NHS Trust

INFORMATION ASSET OWNERS (IAO) HANDBOOK

Asset Owner Handbook 2022 V5
Data Security & Protection

University Hospitals of North Midlands NHS Trust

Contents

1. Introduction - Why do we need an Information Asset Register?

The management of information assets is crucial in achieving a secure information handling and management structure within the Trust. Information is an invaluable resource to the Trust, its loss or misuse can damage its reputation and service delivery, and cause potential harm or distress to individual subjects.

The Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty to comply with guidance issued by the Department of Health (DoH), Information Commissioner's Office (ICO), the Health and Social Care Information Centre (HSCIC), The Information Governance Alliance (IGA) and other advisory groups and professional bodies that provide guidance to staff.

The Data Protection Act is the UK legislation that sets out the rules for processing information of identifiable living individuals. These rules are categorised under eight key principles which organisations collecting or processing data must adhere to as part of their responsibilities as a *data controller* or *data processor*. Appendix A

Under the Data Protection Act/ General Data Protection Regulation (GDPR) the ICO may, in certain circumstances enforce a monetary penalty notice between 10 million and 20 million euros.

Department of Health Information Governance policies and standards require:

"All NHS organisations need a clear Information Risk Management Policy"

And that

"Information Risk management should be a fundamental component of the organisations overall business risk management framework"

Compliance requirements of the National Policy 'NHS Information Risk Management' (NHS Connecting for Health, Digital Information Authority; January 2009 Guidance) is to have knowledge of:

- What information assets we have
- Where they are
- What they hold
- How they are used
- Identify risks

In order to achieve compliance, a register of all information assets has been established, in addition to a review and update programme. This will require ownership and regular administration hence, the necessity for the Information Asset Owner role.

2. What is the purpose of the handbook?

The aim of the handbook is to provide Information Asset Owners (IAO's) with a reference point and provide some practical guidance on:

- Identifying information assets
- Responsibilities of the role
- Managing information risks
- Who can help you

3. What is an information asset?

Types of Assets

An information asset is a body of information, defined and managed as a single unit so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. An asset can be patient, staff or corporate information/data processed by the Trust and held in various forms including paper copies, excel databases and system applications.

Examples of information assets used by the Trust are:

- Electronic Patient Records e.g. Medway, Cris, IPortal
- Paper Health Records
- Images i.e. photographs, x-rays, MRI's
- CCTV recordings
- Audit records

Some simple questions which can help to define if the information held is an asset are:

- Is it of value to the Trust?
- Would there be legal, reputational or financial repercussions if you couldn't produce the information on request?
- Would it have an operational impact if the information could not be accessed or there was a delay in access?
- Is there a risk associated with it? Losing it, being tampered with inappropriate disclosure?
- Will it cost money to reacquire the information?
- Does the group of information have a specific content not held elsewhere?

Further examples of types of assets can be found in Appendix B

Asset Valuation

Assets differ in both format and their importance to Trust business processes. The Trust therefore needs to define the level at which each asset is valued and whether the system level assessments and reviews are appropriate. The Trust's Information Asset Register currently categorises assets as Primary or Secondary assets.

Primary Asset

A primary asset is one which the Trust is reliant on and cannot operate without. The result of the information asset being unavailable for up to 24 hours will disrupt and have an effect on patient care, quality of service and the operations of the Trust.

- Primary information mainly comprises:
- Vital information for the exercise of the organization's mission or business
- Highly Sensitive Information
- Personal information, as can be defined specifically in the sense of the national laws regarding privacy
- Strategic information required for achieving objectives determined by the strategic orientations
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

Secondary Asset

A secondary asset is one which if compromised the Trust as a whole is not reliant on to function however it does perform a necessary localised function. Information held in the asset is personal information or less sensitive information. Secondary assets will often inherit controls implemented to protect the processes and information identified as sensitive (Encryption, Access control etc.).

4. Roles and Responsibilities

Chief Executive

The Trust's Accounting Officer is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks are handled in a similar manner to other risks such as financial, legal and reputational risks.

Senior Information Risk Owner (SIRO)

The SIRO is usually an Executive or senior manager on the Board who is familiar with information risks and the organisations response to risk. The role is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk.

The Trust's Director of IM&T currently holds the SIRO responsibilities.

Caldicott Guardian

The Caldicott Guardian is the person with overall responsibility for protecting the confidentiality of personal identifiable data (PID). The Caldicott Guardian plays a key role in ensuring that the Trust and any third party organisations abide by the highest level of standards for handling PID.
The Trust's Medical Director currently holds the Caldicott Guardian responsibilities.

Data Protection Officer (DPO)

The role of the DPO is to inform and advise the Trust on its obligations under GDPR, monitor regulation compliance and act as an impartial contact for the ICO and individuals (patients or staff) regarding enquiries/breaches relating to data processing, consent, accessing personal data and right to be forgotten. Any information asset data breaches need to be reported to the DPO as well as the SIRO by the Information Asset Owner immediately to ensure that investigations have been implement and the Information Commissioner's Officer have been notified within 72 hours of the breach.

The role of the Data Protection Officer is currently held by the Head of Data Security and Protection.

Information Asset Owner (IAO)

An IAO is usually a senior operational member of staff who is nominated as responsible for one or more identified information assets within the Trust due to their detailed knowledge of the electronic or manual system.

While guidance can be provided to the IAO from Clinical teams who have knowledge of the asset the role of IAO cannot be filled by a Clinical staff member.

The Information Asset Owner is responsible for ensuring that information is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards apply. The IAO provides a common, consistent and unambiguous understanding of what information is held, how important it is, how sensitive it is, how accurate it is, what consent protocols are in place and how reliant the Trust are on it. This helps to ensure the Trust uses the information it needs to operate transparently and accountably.

IAO's are expected to work closely with other IAO's of the Trust to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities, especially where information assets are shared by multiple services.

The IAO's will support the SIRO in their overall information risk management function by providing asset assurance documentation which is compiled for Executive Board review. The six key aspects of the IAO role are:

1. Lead and foster a culture that values, protects and uses information for public good, including responding to access requests.
2. Know what information the asset holds, and what information is transferred in or out of it.
3. Know who has access and why, and ensure that their use of the asset is monitored.
4. Understand and address risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are appropriately managed and reported within 72 hours to the Information Governance team and the Data Protection Officer.
5. Ensure any new information assets or modifications altering the usage of data held in an asset complete a privacy impact assessment (DDPIA) and the asset is logged on the Information Asset Register.
6. The completion of Information Asset Owner training.

The Information Asset owner is responsible for ensuring continuous ownership of all their assigned information assets. If an asset owner is leaving their post or is no longer the most relevant person to

perform this duty then they must contact the SIRO and the Information Governance Team notifying them of the change, nominating a new person to take up that role.

For a complete breakdown of an Information Asset owner responsibilities refer to Appendix C.

Information Asset Administrators

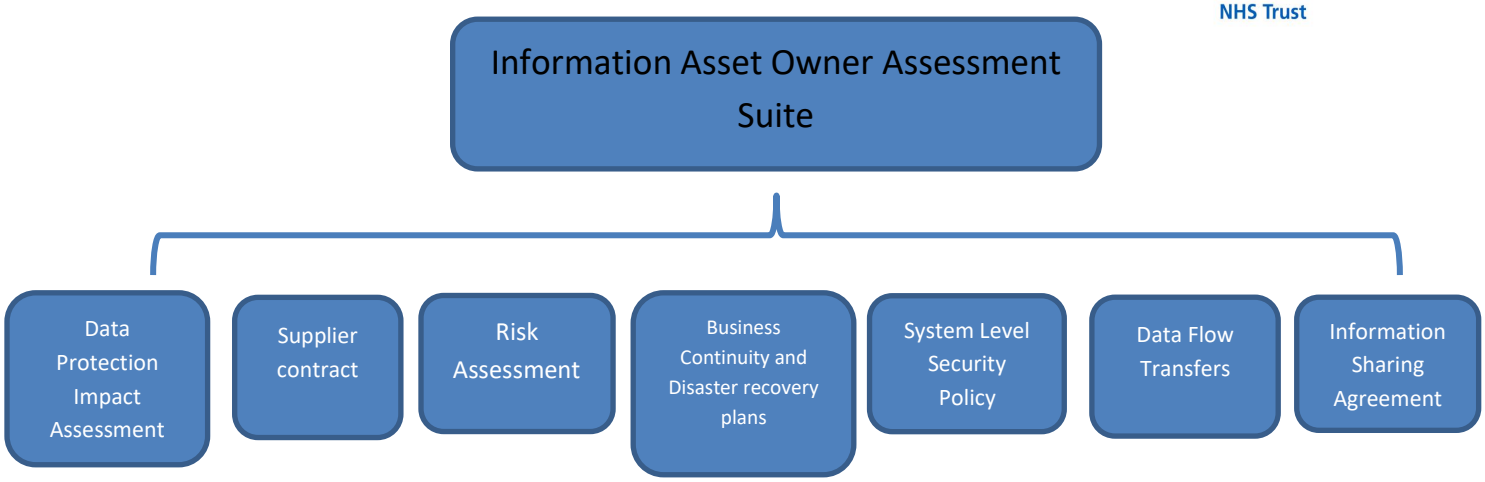
Information Asset Administrators are usually operational members of staff who understand and are familiar with the information asset within their area. Their primary role is to support the IAO to fulfil their duties by taking on the following responsibilities:

- Manage the general data quality of the asset and report areas of concern to the IAO
- Ensure that personal information is not unlawfully exploited, under the direction of the IAO
- Recognise potential or actual security incidents and consult the IAO and record incident on Datix
- Under the direction of their IAO ensure that information is securely destroyed when there is no further requirement for it
- Ensure compliance with information sharing agreements with the local area
- Ensure access to the asset are monitored and applied correctly and refer any difficulties to the IAO.

5. Information Asset Owner Assessment Suite

In order to assist Information Asset Owners in performing the necessary reviews of their assets a suite of assessment forms have been created covering the core elements of Information Security. The forms exist electronically on a SharePoint site and are to be completed or reviewed annually by the IAO. In completing these forms the asset owner will gain an understanding of an asset's compliance against each measure and identify any risks associated with that system. IAOs are responsible for ensuring any risks identified are raised & managed appropriately within their department (Directorate Manager, Working groups etc.).

Information from the forms is viewed by the Trusts' Expert Panel chaired by the Trust's Information Risk Officer, the results of which are provided to the Information Governance Steering Group, jointly chaired by the Trust's SIRO and Caldicott Guardian. Feedback from the Expert Panel may also be relayed to the IAO for further action. The reports are also fed into the Trusts Information Governance Toolkit Submission for the DoH.



Data Protection Impact Assessment (DPIA)

A DPIA is a process which assists the Trust in identifying and minimising the privacy risks of new projects or to review an existing system when the data is being used for purpose other than its original intent. A DPIA enables the Trust to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, this in turn ensures the organisation implements effective standard operating procedures and policies.

The assessment acts as a check list to ensure that the information asset has accounted for all aspects of information security. The answers to the DPIA will assist in the completion of the remaining IOA assessment suite documentation. The DPIA helps the IAO or project manager to review the benefits that information sharing might bring to the trust, specific individuals or society as a whole. It also helps to assess any risks or potential negative effects, such as risks to confidentiality that may cause potential harm, distress or embarrassment to individuals or the Trust's reputation if information is shared inappropriately.

After the initial completion the DPIA does not need further review unless it is likely to involve a new use or significantly change the way it handles personal data. Any major changes to information assets must be agreed, this includes new and or replacement software, system updates and installations, removal or archiving of an information asset and the creation of a new information asset.

Contract

When the Trust acting as data controller uses an external company to act as processor, there must be a written contract (or other legal act) in place. The contract is important so that both parties understand their responsibilities and liabilities. If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.
The contract (or other legal act) sets out details of the processing including:

- The subject matter of the processing
- The duration of the processing
- The nature and the purpose of the processing
- The type of personal data involved
- The categories of data subject
- The controller's obligations and rights

Risk Assessment

It is an Information Governance requirement that a risk assessment is conducted on the information asset on an annual basis as a minimum. Any actual or perceived risk must be discussed at divisional level and considered for inclusion on the Divisional Trust Risk Register (DATIX). The assessment template has been created in line with the Trust's RM01 Risk Management Policy and Strategy. See Appendix E for examples of Information risk.

Business Continuity and Disaster Recovery

Business continuity is a core component of corporate risk management and emergency planning. Its purpose is to counteract or minimise interruptions to a Trust's business activities from the effects of major failures or disruptions to its information assets.

Within the NHS there is a large amount of information that needs to be kept secure; however, the way that we secure this information must not have a negative impact on healthcare.

Therefore, in order to save lives and provide continued healthcare in the event of a disaster or incident, the solution to enable business and service continuity in some instances may not be deemed as secure as before. However, what must be stressed is that an approach with a blatant disregard for security should not even be considered as there is still a responsibility for patient safety and confidentiality. Security needs to be flexible, for within the NHS clinical safety will be the priority. In a disaster situation issues surrounding clinical safety will always take precedence over security issues.

System Level Security Policy

The development, implementation and management of the System Level Security Policy (SLSP) will demonstrate an Information Asset Owners understanding of information governance risks and commitment to addressing the security and confidentiality needs of a particular system. An effective SLSP therefore contains a considered and specific view of the range of security policy and management issues relevant to a system and encompass a range of technical, operational and procedural security topics.

The SLSP identifies appropriate lines of accountability, both within the Trust and for those other bodies who may legitimately use it. The SLSP includes references to other external security documentation and standards, including the Trust's corporate security policy and where relevant, the security policies and procedures of other organisations. Where the system is available to multiple organisations, the SLSP must establish the necessary common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

The SLSP is a core component of an accreditation documentation set for those organisations that undertake formal accreditation processes for their information assets. NHS organisations are required as part of the Information Governance requirements to generate SLSP for all / major / critical information systems.

Data Flow Transfers

This is the process of documenting a regular exchange of data/information from one location/system to another and the method by which it is exchanged. Data flows may include; system to system transfers, email, fax, post/courier, text or portable electronic or removable media.

A key element of the data flow transfer map will be to identify if the asset is transferring data to other countries. If an "overseas" transfer is identified the Information Asset Owner must contact the Information Governance team to complete the Trust's Overseas Data Proforma. Information sent outside of England and Scotland is classed as high risk and the Trust must ensure appropriate security arrangements are in place. European countries and the rest of the world have different data protection laws than the UK, but from May 2018 with the new GDPR legislation there will parity across all of Europe.

Typical terminology used for data flow mapping;

Terminology	Description
Inbound Flow	Information/data being received by the asset
Outbound Flow	Information/data being sent from the asset
External Flow	Information transfer flow between the asset and third party
Pseudonymised data	Data that appears anonymous to the person receiving it but contains a code that will allow those sending the data to identify the individual from it.
Anonymised data	Information that cannot identify anyone
Bulk Data	The data contains identifiable data on more than 50 individuals
Personal data	Includes individuals name, date of birth, postal address
Sensitive/Special category data	Data relating to race/ethnicity, political opinions, religious beliefs, trade union status, physical/mental health, sexual orientation, criminal offence, genetic/biometric data (gene sequence, fingerprints, facial recognition, retinal scanning etc.)

Information Sharing Agreement

The purpose of an information sharing agreement is to provide a robust method of sharing personal identifiable data between an organisation and another third party data controller when a legitimate purpose for sharing has been identified. The agreement is a set of operational steps that both parties must adhere to regarding the sharing of date. The agreement must outline the following

- the purpose, or purposes, of the sharing
- the legal basis for sharing
- The specific data to be shared
- the potential recipients or types of recipient and the circumstances in which they will have access
- How the information is transferred to the third party
- The security of the data
- The retention of the shared data

Agreed sharing timescales, this may be information shared for a specific period dates or an on-going sharing arrangement. If on-going the agreement should be reviewed annually to ensure that any changes in process are highlighted the agreement reassessed for assurance.

6. Decommissioning

Any system or source of information may be considered an Information Asset even if it is not used regularly or in a 'live' environment. For example, old systems that have been superseded may be kept in order to store and access historic patient information. These assets should still provide the same level of information security assurance and will remain on the asset register as 'live' assets.

Assets remain on the register until the IAO can provide assurance to the SIRO via the Expert Panel that the asset has been fully decommissioned. This may involve (list not exhaustive)

- Uninstalling Software
- Removing Hardware
- Physically destruction of any device or removable storage (hard-drives/flash-drives) Migrating/Archiving Data (transference to Secondary Asset)
- Confirmation/ Sign off from suppliers & Third parties
- End of Information Sharing Agreements

7. Who do I contact if I have questions about an asset or completing the IAO assessment suite documentation?

Please contact the Information Governance Team and ask to speak to

Data Security & Protection Team, DSPUHNM@uhnm.nhs.uk

Appendix A

Data Protection/GDPR Principles

Further guidance on the Data Protection Act/GDPR can be obtained from the Trust's Information Governance Team, Trust Policy for Data Protection Security and Confidentiality (IG10) and for the Information Commissioner's Office (www.ico.gov.uk).

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   a. At least one of the conditions in Article 6 is met; and
   b. In the case of sensitive personal data, at least one of the conditions in Article 9 is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

8) Personal data shall not be transferred to a country of territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B

Types of Information Assets

It is generally sensible to group information assets in a logical manner e.g. where they are all related to the same information systems or business process.

Typical assets include:

Personal Information Content	Software
Databases and data files Back-up and archive data Audit data Paper records (patient case notes and staff records) Paper reports	Applications and System Software Data encryption utilities Development and Maintenance Tools
Other Information Content	**Hardware**
Databases and data files Back-up and archive data Audit data Paper records and reports	Computing hardware including PCs, Laptops, PDA, communications devices e.g. blackberry and removable media. Medical Devices that hold patient/staff clinical data.
System/Process Documentation	**Miscellaneous**
System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Business continuity plans	Environmental services e.g. power and air-conditioning (if personal information is stored by these systems) People skills and experience Shared service including Networks and Printers Computer rooms and equipment Records libraries

Appendix C

Information Asset Owner Responsibilities

Overview	What an IAO needs to do
Lead and foster a culture that values, protects and uses information for public good	• Complete IAO training on appointment. • Actively contribute to the Trust's/ Department's plans to achieve and monitor the right NHS Information Governance culture. • Ensure the handling of your information asset complies with the Data Protection Act and forthcoming GDPR legislation. • Understand and document the business value of the information asset you are responsible for. • To consider whether better use of any information held is possible or whether information is no longer required.
Know what information the asset holds, and what information is transferred in or out of it.	• Understand and address risks to your information asset, and provide assurance to Trust SIRO. • Know who has access to your information assets and why, and monitor use. • Understand whether a delivery partner or supplier has a dependency on your information to deliver a service. • Approve and minimise transfers • Monitor the allocation of users' rights to transfer personal information to removable media like laptops, usb sticks. • Approve arrangements so that information put onto removable media is minimised and protected. • Approve the information disposal mechanisms for the asset
Know who has access and why, and ensure that their use of the asset is monitored.	• Understand the Trust's policies on the use of information and the management of information risk. • Ensure that you keep a record of individuals with administrative access to the system, or who can edit records containing personal data. • Keep a log of access requests • Ensure that the use of the asset is checked regularly and that use remains in line with policy
Understand and address risks to the asset, provide assurance to the SIRO	• To seek advice from information governance subject matter experts when reviewing information risk • To conduct Privacy Impact Assessments for all new projects • To undertake yearly risk assessment reviews for all 'owned' information assets in accordance with NHS Information Governance guidance and report to the SIRO, ensuring that information risks are identified, documented and addressed • To escalate risks to the SIRO where appropriate and to make the case where necessary for new investment to secure 'owned' assets • To provide an annual written assessment to the SIRO for all assets they 'own'.

Appendix D

National Data Guardian - 10 Data Security Standards

Leadership Obligation 1 – People
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit.

Leadership Obligation 2 - Process
Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3 - Technology
Ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

Appendix E

Example Risks relating to Information Security:

A) Confidentiality / Security:

Access Control:

- No access control / shared user accounts are used.
- Password complexity not enforced / criteria does not include minimum of 8 characters / symbols / upper case characters / lowercase characters / numbers.
- No password change period enforced.
- No password history / Password history less than 4 previous passwords.
- Insufficient / No measures in place to protect against brute force i.e. users can make 20 incorrect password attempts.

Security Procedures:

- Procedures not in place to confirm a user's identity before re-setting a password i.e. when request received via telephone.
- Insufficient / No time out period applied
- No management authorisation process built into registration procedure / No system training provided.
- No de-registration procedure in place / User access not revoked for 12 months after a user has left the organisation / De-registration procedures do not account for suspended staff / staff on long term leave. Temporary / dummy / admin accounts used and not set to expire / passwords never changed.

Other Security Issues:

- System hosted externally
- Support organisation provides no / inadequate assurances of data security i.e. no ISO27001 certification / IG Toolkit not completed.
- No adequate contract or SLA in place.
- No independent penetration test undertaken on system server/application.
- Data is processed in data centres which are based outside of the UK.
- No Information Sharing Protocol in place with partner organisations
- No confidentiality agreement in place with supplier / support organisation.
- Staff / Supplier / support organisation requires remote access to the system.
- Data is transferred via email / internet / on removable media without adequate protection i.e. encryption.
- Data is cached / stored locally on unencrypted devices.
- Procedures are not in place to physically secure paper documents / follow up misplaced paper documents.
- Identifiable data used for secondary purposes (statistical reports / research / other).

B) Integrity / Accuracy:

- Administrations / users do not receive appropriate systems training
- System relies on data from [system] i.e. dependencies. Risk of service disruption if [system] fails.
- Supplier not compliant with IG Toolkit/ISO27001
- System not complaint with patient safety risk management alert i.e. not compatible with NHS number
- Supplier / Support organisation not ISO9001 certified.
- System not BS10008 compliant / documents scanned and originals destroyed.
- Monitoring of user audit trails does not take place / too infrequent.
- No / inadequate antivirus/malware.
- Inadequate procedure to investigate confidentiality breach.
- Maintenance - change control procedures inadequate / error log not in place.

C) Availability:

- Resilience measures inadequate / in the event of loss of network / power the system cannot be accessed
- Back-ups not taken daily / back-ups not verified
- Business Continuity / Disaster Recovery Arrangements non-existent / in adequate / not tested etc.