North East Ambulance Service NHS
NHS Foundation Trust

Information Security and Risk Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-7
Version Number	V05
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	12 June 2018
Date Policy Effective From	12 June 2018
Next Review Date	12 June 2021
Keywords	Asset; availability; backup; breach; business continuity; CareCert; controller; confidentiality; consequence; cyber; data; protection; disaster recovery; DPA; DPIA; encryption; forensic; GDPR; hardware; IAA; IAO; IAR; impact; incident; integrity; ISO27001; likelihood; patches; penetration test; processing; personal; processing; recovery; removable media; SIRO; software; special category; system; technical; vulnerability;

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
1	All 4.1 4.2	• Document transferred into new template. • NEAS replaced with 'the Trust'. • 'Monitoring system access and use' section of the policy removed and updated in to section 7. • Do not store personal, sensitive or business information on personal devices or non-Trust systems e.g. Cloud applications without authorisation from the Assistant Director of IM&T. • Ensure that HR (instead of IT Service Desk) are notified of new and leaving employees.	Information Governance Manager	18 Aug 2014
1	EIA	It was suggested that the acronyms EIA and EIS should be expanded for clarity (to Equality Impact Assessment and Equality Impact Screening) – cannot change as this is part of the template.	Information Governance Manager	22 Sep 2014
1	All	Proof read following comment from Compliance & Risk Committee.	Information Governance Manager	16 Oct 2014
3		Q-pulse numbering changed due to restructuring of the system and review date set at previous revision and table of revision amended to reflect change along with version numbers		19 Jan 2016
4	All	Reformat into new template	Information Governance Manager	Oct 2016
5	All	Full review of Information Security Policy with elements of information risk added and policy renamed. GDPR requirements included. Grammatical updates. Revision ISWG duties. Additional training requirements under section 7.	IG Manager Informatics Manager Network and Telephony Officer	Mar 2018 Jun 2018 Jun 2018

This page should not be longer than one single page.

Table of Contents

1. Introduction

This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards under the UK Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR).

An effective information security management regime ensures information is properly protected and is reliably available. Without effective security, the Trust's information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised parties.

High quality information underpins the delivery of high quality evidence-based healthcare and many other key service deliverables. Information has the greatest value when it is accurate, up to date and is accessible where and when it is needed.

Effective information security management is underpinned by robust information risk management processes. These processes requires the Trust to have a robust information risk management structure in place that reduces risks and threats to information whilst retaining its security, availability and accessibility.

2. Purpose

The purpose of this document is to set out a framework under which the policy will preserve confidentiality, integrity and availability of information. It provides guidance on how to protect, to a consistently high standard, all information assets, including manual and electronic records, both patient and other Trust corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

3. Scope

This policy covers both the Trust (North East Ambulance Service NHS Foundation Trust) and its subsidiary company North East Ambulance Service Unified Solutions (NEASUS). References to NEAS or Trust within this policy also cover NEASUS and its employees.

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, volunteer or contractor.

Other agencies and individuals working with the Trust, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments / sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information security and risk management processes are providing them with adequate and appropriate assurances relating to risks against the Trust's objectives. The Trust as a body corporate is the data controller.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility. The SIRO also acts as an advocate for information risk on the Board and in internal discussions and provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

4.4 Directors

Each Director will be designated with risk / data ownership for information assets under their control at Directorate level and they will in turn identify Service / Departmental Risk / Information Asset Owners (IAOs).

4.5 Information Asset Owners

- Undertaking an information governance review of all assets during procurement and at least annually (see Guidance for Contracting a Data Processor).
- Knowing what information comprises or is associated with the asset, what enters and leaves it and why.
- Knowing who has access to the asset, whether system or information, and why, and ensuring access is monitored and compliant with policy.
- Understanding and addressing risks to the asset, and providing assurance to the SIRO.
- Ensure information assets are logged on the Trust Information Asset Register (IAR).

4.6 Information Asset Administrators (IAAs)

Responsible for day-to-day management of information risk for their asset on behalf of the IAO.

4.7 Information Governance Manager

- To provide lead specialist advice on information security in line with ISO27001 and CareCERT.

- To provide specialist advice for assessing the adequacy and co-ordinating the implementation of specific controls for new systems, products or service.
- To manage the creation and maintenance of the information asset register.
- To assist The Trust to carry out initial information assets risk assessments.
- To manage the investigation and reporting on security incidents when requested by The Trust, including establishing causes and determining appropriate corrective and/or preventive action, and report recommendations and corrective actions directly to the Trust.
- Promote a data security and data quality improvement culture throughout the organisation to ensure integrity and accuracy of information, available at the point of care that is available for management, planning and statutory reporting obligations.

4.8 Information Security Working Group (ISWG)

- Monitor for actual or potential information security breaches.
- Report information security issues in line with the group's Terms of Reference.
- Understand the risk to the computer assets and the information that is held on them.
- Implement specific security measures where personal information is being transferred whether manually or electronically e.g. using portable computers, USB etc.
- Commission penetration testing to ensure network and system security.
- Ensure back up procedures are established and maintained.
- Ensure appropriate revision of antivirus software and patches are installed on all servers and PCs.
- Ensure that PCs, servers and other relevant hardware is disposed of securely in accordance with disposal legislation.

4.9 All staff

All staff are responsible for ensuring that the principles outlined within this policy are universally applied. Compliance with information security is the responsibility of all members of the Trust who process personal information and include contractors, temporary staff and students. Members of the Trust are responsible for ensuring that any personal data supplied to the Trust are accurate and up-to-date.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Consequence	The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or

Term	Description
	password.
Hardware	In Information Technology is a physical device such as a VDU or printer.
Impact	The adverse change to the level of business objectives achieved.
Information Assets (IA) and registers	Are identifiable and definable assets owned or contracted by an organisation which are valuable to the organisation. The registers will likely include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data.
Information Asset Administrators (IAA)	Support the IAO to ensure that this procedure is followed, recognise actual and potential security incidents, and consult the appropriate IAO on incident management
Information Asset Owners (IAO)	Are senior individuals within the Trust IAOs accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned assets.
Information Security Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. It is measured in terms of the likelihood of an event and its consequence.
Likelihood	A qualitative description or synonym for probability or frequency.
Patches	Are updates to computer programs, such as anti-virus, to keep the program up to date or to fix a bug within a program.
Personal Data	Information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Removable media	Is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs / DVDs, USB flash memory sticks or pens, PDAs.
Risk	Can be defined as the chance that something will happen that will have an adverse impact on the achievement of the Trusts aims and objectives. It is measured in terms of consequence and likelihood.
Risk management	Is concerned with ensuring that risks are recognised and their impact on the Trust is assessed in order that the appropriate resource can be channeled to minimise or eliminate any potential loss.
Risk management process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating,

Term	Description
	monitoring and communicating risk.
Software	Are programs that run on a computer e.g. word-processing software, spreadsheets etc.
Special category data	Special category data is more sensitive, and so needs more protection. For example, information about an individual's: • race; • ethnic origin; • politics; • religion; • trade union membership; • genetics; • biometrics (where used for ID purposes); • health; • sex life; or • sexual orientation.
System or data	Used in the context of this policy refers to all information held in either electronic or paper format, also an "information asset" is a definable piece of information stored in a manner which is recognised as 'valuable' to the Trust.
USB, universal serial bus	Or port connection that is universally compatible with many types of device such as wireless, printers, memory sticks etc.

6. Policy Content

6.1 GDPR security principle

The GDPR requires us to process personal data securely. It mandates how to assess information risk and put appropriate security measures in place. Article 5 (1f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be:

'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

Information security is sometimes considered as cybersecurity (the protection of networks and information systems from attack), it also covers other things like physical and organisational security measures.

This security principle needs to be considered alongside Article 32 of the GDPR, which provides more specifics on the security of processing. Article 32(1) states:

'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and

severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'

Information security supports good data governance and will demonstrate our compliance with other aspects of the GDPR.

6.2 Data protection by design

Alongside the security principle, the GDPR makes data protection by design a legal requirement. Article 25 mandates that, at the time of the determination of the means of the processing (i.e. the design phase of any processing operation) and at the time of the processing itself, you should put in place appropriate technical and organisational measures designed to implement data protection in an effective manner and to integrate the necessary safeguards into the processing.

Whether you are a controller or a processor, you also have specific security obligations under Article 32 of the GDPR. These require you to put in place appropriate technical and organisational measures to ensure a level of security of both the processing and your processing environment. IAOs are responsible for liaising with the Head of Contracts and Procurement when identifying the need to procure goods/service from a commercial organisation and ensure the contract contains the specific requirements relating to the processing of personal information (see Guidance for Contracting a Data Processor).

6.3 Confidentiality, integrity, availability

Collectively known as CIA, confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for NEAS as a data controller, and for the individuals whose data is processed.

The security measures the Trust puts in place should seek to ensure that:

- The data can be accessed, altered, disclosed or deleted only by those authorised to do so.
- The data is accurate and complete in relation to why it is being processed.
- The data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, it should be recoverable and therefore prevent any damage or distress to the individuals concerned.

Examples include **business continuity plans, disaster recovery, and cyber resilience.** GDPR requires us to have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a 'timely manner'. There must be an appropriate backup process in place to restore systems, and therefore the personal data they hold, as soon as reasonably possible.

6.4 Risk management

GDPR emphasises a risk-based approach to data protection and the security of the processing systems and services. You must take steps to assess these risks and include appropriate organisational measures to make effective risk-based decisions

based upon:

- The state of the art (of technology).
- The cost of implementation.
- The nature, scope, context and purpose of processing.
- The severity and likelihood of the risk(s).

Beyond this, where the processing is likely to result in a high risk to the rights and freedoms of individuals, you must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, you need to have a process in place to consult with the ICO before you start the processing (see Guidance for Contracting a Data Processor – Information Governance System Review).

Once identified, information security risks will be managed on a formal basis through the Information Governance Risk Register and monitored by the Information Security Working Group. Risks will be recorded within a Trust risk register and action plans will be developed to demonstrate the Trust's effective management of its information assets risks.

6.5 Information assets

The Trust Information Asset Register (IAR) will be managed and maintained by the Information Governance Manager in liaison with the Trust's IAOs. As a minimum priority will be given to information assets that (a) contain personal information about patients or staff and/or (b) are essential to the support of Trust operations, e.g. financial systems, infrastructure documentation.

6.6 Data processors

Where a third parties data processor is used, the Trust IAO must ensure that they employ appropriate security measures (see Guidance for Contracting a Data Processor - Third Party Due Diligence Assessment). The GDPR includes provisions where processors are used, including specific stipulations that must feature in the contract (Guidance for Contracting a Data Processor – Data Protection Protocol).

6.7 Identity and access control

Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed (see Domain Account Policy).

IAO need to ensure:

- They undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.
- Users that have privileged access are strongly authenticated and consider two-factor or hardware authentication measures.
- Users are prevented from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. You

should appropriately constrain legitimate access and ensure there is an appropriate audit trail.
- There is a robust password policy which avoids users having weak passwords, such as those trivially guessable. You should change all default passwords and remove or suspend unused accounts.

6.8 Technical measures

Technical measures include both physical and computer or IT security. When considering physical security, you should look at factors such as:

- The quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV.
- How you control access to your premises, and how visitors are supervised.
- How you dispose of any paper and electronic waste.
- How you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. When considering cybersecurity, you should look at factors such as:

- Tracking and recording all assets that process personal data, including end user devices and removable media.
- Minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity.
- Actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), and taking other mitigating steps, where patches can't be applied.
- Managing end user devices (laptops and smartphones etc.) so that you can apply organisational controls over software or applications that interact with or access personal data.
- Encrypting personal data at rest on devices (laptops, smartphones, removable media) that are not subject to strong physical controls (see Data Encryption Policy).
- Encrypting personal data when transmitted electronically (see Secure Transfer of Information Policy).
- Ensuring that web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications such as the OWASP Top 10.
- Advice from CareCERT bulletins.
- Adopting basic safeguards to prevent users from unsafe internet use e.g. anti-virus, anti-spam filters and basic firewall.

You also undertake regular testing to evaluate the effectiveness of your security measures, **including virus and malware scanning, vulnerability scanning and penetration testing as appropriate**. The results of any testing and remediating action plans should be monitored.

6.9 Vulnerability scanning and penetration testing

These are essentially 'stress tests' of the network and information systems, which are designed to reveal areas of potential risk and things that can be improved. GDPR

specifically requires a process for regularly testing, assessing and evaluating the effectiveness of any security measures put in place.

6.10 Incident management

All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. All Trust incidents must be reported using the Trust incident reporting procedures and managed in line with the Trust's Incident Reporting Policy.

Article 33(1) of the GDPR requires:

'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'

Where there is an information security breach or event this will be managed by the Information Governance Manager and reported to the SIRO. The ISWG will review reported information security incidents and where applicable approve changes to Trust policies and procedures to reduce the risk of the information security incident reoccurring.

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious, and could be reported as a Serious Incident. This applies irrespective of the media involved and includes both the loss of electronic media and paper records.

6.11 Business continuity planning

All business continuity plans (BCPs) must include detail how they will respond to threats to data security, including significant data breaches or near misses. IT are responsible for undertaking a formal risk assessment in order to determine the requirements for IT Business Continuity and a Disaster Recovery Plan which in liaison with the Trust's Business Continuity and Disaster Recovery covers all essential and critical business activities.

All plans should be regularly tested. The outcome of the tests should be used to inform the future development of the incident management plans. The preservation and analysis of the sequence of events that led up to the incident is critical to identify and remedy the root cause.

Conduct a lessons learned review: Log the actions taken during an incident and review the performance of the incident management process post incident (or following a test) to see what aspects worked well and what could be improved.

6.12 Back-up, recovery and archiving

The Trust's IT department is responsible for backing up the Trust servers on a daily basis in accordance with the Trust's back up procedure.

Staff using laptops or portable computers must ensure that these are connected to the

network at least once a month to ensure that the software on the laptop is kept up to date and ensure information held is backed up (e.g. via offline folders and files).

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved (e.g. means to read and recover the information must be available during the expected life of the store information).

The archiving of electronic data files must reflect the needs of the Trust and any legal and regulatory requirements.

6.13 Forensic readiness

The universal use of IT systems in the Trust leads to the need to have digital evidence available for a wide range of investigations or disputes e.g. patient confidentiality breaches, security incidents, criminal activities, commercial disputes, disciplinary actions and privacy issues.

These disputes present a risk to the Trust's information assets, which without adequate mitigation could damage the Trust's business or undermine the reputation of the Trust.

Where the Trust identifies a need to undertake a Forensic examination, the Trust's SIRO, in liaison with the Trust's Counter Fraud Office will authorise such an assessment utilising the services of a commercial IT Forensic company.

7. Training Required for Compliance with this Policy

All staff to receive mandatory data security training on an annual basis. Additional security training will also be provided based on trends from information security breaches. Additional relevant training will also be undertaken by the SIRO, IAOs and members of the ISWG.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work

Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	Number of data/cyber security incidents/breaches/complaints to ICO.
When will the monitoring be performed?	Every other month.
How are you going to monitor?	Via Ulysses reports.
What will happen if any shortfalls are identified?	Logged in risk registers.
Where will the results of the monitoring be reported?	Information Security Working Group.
How will the resulting action plan be progressed and monitored?	The action plan will be progressed and monitored by the Information Governance Working Group. Incident trends will be identified to formulate internal training courses.
How will learning take place?	Learning will be via the action plans and monitored by Information Governance Manager.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Monitoring and reporting on Policy compliance	Number of data/cyber security incidents	Via Safeguard reports	Information Governance Manager	ISWG	Bi-monthly	Add to risk registers

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with the Information Governance Working Group, ISWG, SIRO and Executive Directors.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- UK Data Protection Act (DPA)
- EU General Data Protection Regulation (GDPR)
- ISO27001
- CareCERT

13. Associated Documentation

This policy refers to the following Trust documents:

- Data Protection Policy – POL-F-IMT-4
- Domain Account Policy – POL-F-IMT-5
- Guidance for contracting a Data Processor – QSSD-F-IG-1
- Data Encryption Policy – POL-F-IMT-2
- Secure Transfer of Information Policy – POL-F-IMT-11