South East Coast Ambulance Service NHS
NHS Foundation Trust

Removable Media: Information Security Policy

Contents

1 Introduction

1.1. The South East Coast Ambulance Service NHS Trust (the Trust) recognises its responsibility to ensure the confidentiality, integrity and availability of the information it holds and the increased risk to the security of data that is stored on removable media.

1.2. This policy sets out the measures required to mitigate these risks where removable media are used.

1.3. The objective of this policy is to prevent unauthorised disclosure, modification, removal or destruction of Trust's information assets; patient and staff related information and disruption to Trust's business activities.

2 Aims and Objectives

2.1. The aim of this document is to prevent the unauthorised disclosure, modification, removal or destruction of sensitive or confidential information through the unregulated use of removable media.

2.2. The objective of the document is to lay down clear guidelines as to how sensitive and confidential data can be safely transported when the only option available is to use removable media.

3 Definitions

3.1. For the purpose of this policy, removable media is defined as:

3.1.1. All recording media including tapes, floppy discs etc.

3.1.2. Removable or external hard disc drives.

3.1.3. Optical discs, DVD and CD-ROM.

3.1.4. Any new technology which acts as removable media.

3.1.5. Solid state memory devices including memory cards, USB devices and pen drives etc. that are not permanently attached to a desktop or laptop computer.

3.1.6. USB devices which are used for accessibility purposes which, might maintain recorded data.

4 Policy Statement

4.1. The use of removable media within the Trust will only be allowed under strictly controlled conditions. Only devices that have been authorised or dispensed by the Trust's IT department must be utilised with the Trust IT equipment. As a standard these will be encrypted and only accessible with a PIN.

4.2. USB devices used for accessibility purposes must be approved for use by the Trust's IT Security team and Information Governance function before being authorised/purchased.

5 Arrangements

5.1. All sensitive and confidential information will be stored to an appropriate location on the Trust network, or cloud service provided by the Trust for this purpose such as Office365, which has role-based access controls. The network can be accessed from any Trust location. However, it is recognised that there are exceptional circumstances that may arise where information needs to be transported to other locations. If removal media is to be used, the following directives need to be applied:

5.1.1. Personal, sensitive or otherwise confidential information must only be stored on Trust approved removable media which is encrypted.

5.1.2. Removable media shall only be used by staff and contractors who have an identified and agreed business need for them. This business need shall be agreed by the relevant Information Asset Owner (IAO).

5.1.3. The use of removable media by sub-contractors or temporary workers must be risk assessed and be specifically authorised by IT.

5.1.4. The Information Asset Owner (IAO) within each business area shall identify its need for removable media and the devices on which removable media are to be used.

5.1.5. Removable media that have been approved for use within the Trust will be appropriately identified as such and a record held by the Information Asset Administrator (IAA).

5.1.6. Removable media may only be used to store and share NHS information that is required for a specific business purpose.

5.1.7. When the business purpose has been satisfied, the contents of removable media must be removed from those media through a destruction method that makes recovery of the data impossible. Alternatively, the removable media and their data must be destroyed and disposed of securely in such a way that prevents potential reuse. Guidance must be sought through the IT Security Manager regarding disposal. In all cases, a record of the action to remove data from or to destroy data must be recorded in an auditable log file.

5.1.8. Removable media must not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained by the IAA of all removable media taken or sent off-site or brought into or received by the Trust. This record must also identify the data files involved.

5.1.9. Removable media must be physically protected against their loss, damage, abuse or misuse when used, in storage or in transit.

5.1.10. Data archives or back-ups taken and stored on removable media, either short-term or long-term, must take account of any manufacturer's specification or guarantee and any limitations therein.

5.1.11. Audit spot checks will be conducted by the IAOs to ensure compliance with this policy. Any non-compliance issues will be reported to the line managers concerned and may be handled through staff disciplinary processes or contractual arrangements.

5.1.12. All incidents involving the use of removable media must be reported to the Trust's Head of Information Governance / Information Governance Manager immediately and in accordance with the Trust's Incident Reporting Policy (Datix) & Procedure.

5.1.13. The Trust reserves the right to introduce additional technical controls, such as blocking or restricting use of USB ports, at some future point. However, such introduction will be properly communicated, as appropriate.

6 Responsibilities

6.1. Information Asset Owners (IAOs) have overall responsibility for all data held on their systems and will decide if the use of removable media to copy, update or remove data is appropriate and applicable.

6.2. Information Asset Administrators (IAAs) have the responsibility to maintain a record of all removable media and identify the data files involved.

6.3. Staff and contractors are not permitted to introduce or use any removable media other than those provided or explicitly approved for use by the Trust.

6.4. Any bulk extracts of confidential or sensitive data must be authorised by the responsible Director for the work area.

6.5. Only removable media supplied and controlled by the IT Team will be used for the movement of Trust information.

6.6. The IT Security Manager is responsible for identifying and implementing any device configuration requirements that the Trust may require in order to comply with NHS IG security policy and standards. This includes data encryption capabilities.

6.7. Line managers, in collaboration with the IT Security Manager, are responsible for the day-to-day management and oversight of removable media used within their work areas to ensure this policy is followed.

6.8. Information Asset Administrators are responsible for the secure storage of all unallocated removable media and their related control documentation as required by this policy.

6.9. Staff who have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as required by this policy. Failure to comply with this removable media policy may endanger the Trust's information services and may result in disciplinary or legal action.

6.10. Staff involved in data extraction and data file creation must receive appropriate Information Governance training.

6.11. Staff must be aware of policy and procedure governing the work area including consequences of breach of policy.

7 Competence

7.1. The directives laid down in this policy apply to all Trust staff.

7.2. The Corporate Induction course will raise awareness of security and confidentiality issues for all new entrants.

7.3. Statutory IG training is completed on an annual basis, this provides awareness of security and confidentiality.

7.4. The IT Service Desk Team will brief laptop users on the safe transportation of sensitive and confidential data as part of the handover process of the laptop.

7.5. Existing staff will be advised of the need to be aware of data security and confidentiality and the directives contained in this document through items regularly entered in the Trust Bulletin, Team Briefing Folders and published on the Trust Intranet.

7.6. Information Security and Confidentiality sessions, including Removable Media: Information Security will be included in the Clinical Refresher Training Sessions.

8 Monitoring

8.1. The Information Security and Registration Authority Manager (ISRAM) will report on any breaches in security or near misses, and compliance with the policy to the Information Governance Working Group (IGWG).

9 Audit and Review

9.1. The IGWG will review at each meeting any security breaches, trends or near misses to ensure adherence to this policy. Where applicable,

the IGWG will oversee the development of action plans to address any deficiencies.

9.2. The Board may request the Trust's Internal Auditors to carry out an information security audit from time to time, to seek further assurance that this policy is robust.

9.3. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

9.4. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

9.5. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

9.6. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

10 References

- Data Protection Act 2018
- UK General Data Protection Regulation. 2021
- General Data Protection Regulation 2016
- Computer Misuse Act 1990
- ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management
- Information Security Management: NHS Code of Practice