Reti Health - Information Security Policy

Contents

Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Reti Health by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies
- Working with other partners to develop collaborative approaches, systems and processes relating to information security
- Describing the principles of security and explaining how they are implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.

Roles and Responsibilities

Chief Executive Officer (CEO)

Responsibility for information security resides ultimately with the Chief Executive Officer. This responsibility is discharged through the designated role of Chief Technology Officer.

Chief Technology Officer (CTO)

The Chief Technology Officer is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure Reti Health's systems and infrastructure remain compliant with the Data Protection Act 2018, and to ensure industry security best practices are upheld when dealing with personal data.

Data Protection Officer (DPO)

The General Data Protection Regulation (GDPR) requires us to appoint a Data Protection Officer (DPO). The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters.

All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. In particular all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected breach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Chief Technology Officer.

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or subcontractors of the external organisation comply with all appropriate security policies.

Policy Framework

Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the CTO.

Computer Access Controls

Access to Reti Health computers shall be controlled and restricted to those authorised users who have a legitimate business need. This will also require agreed systems and processes with third party vendors working for and on behalf of Reti Health.

All computers shall be password protected and have hard drives encrypted while at rest. Computers shall be physically protected from threats at secure offices, staff homes, or by staff when being transported.

Cloud Service Provider Access Controls

Cloud services, including cloud computing, email providers, and other cloud software providers shall be approved by the CTO before operation is commenced. Wherever possible, multi-factor authentication shall be used.

Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Equipment Security

In order to minimise loss of, or damage to, all assets, the CTO shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

Information Security Events and Weaknesses

All Reti Health information security events, near misses, and suspected weaknesses are to be reported to the CTO and where appropriate reported as an adverse incident. All adverse incidents shall be reported to the DPO.

Protection from Malicious Software

The organisation and its service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to cooperate fully with this policy. Users shall not install software on the organisation’s property without permission from the CTO. Users breaching this requirement may be subject to disciplinary action.

Removable Media

All removable media must be encrypted. Removable media containing software require the approval of the CTO before they may be used on Reti Health systems. Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. Reti Health will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks are approved by the CTO before they commence operation.

System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CTO.

References

The NHS England Information Security Policy has been used as template for the creation of this document

Legislation

- The Data Protection Act (2018)
- The General Data Protection Regulation
- Regulation of Investigatory Powers Act (2000)