Cyber & Information Security Policy (Statement)

We (Elysium Healthcare) are committed to the highest standards of cyber and information security. Protecting the information of our patients, colleagues, and partners is central to delivering safe and effective care.

Our Commitment

We are committed to:

- Protecting the confidentiality, integrity, and availability of information across all our hospitals, care homes, and services.
- Ensuring information is accessible only to those who need it, when they need it.
- Protecting information from accidental or deliberate compromise, whether by internal or external threats.
- Operating centrally managed systems and networks that are secure, resilient, and compliant with UK GDPR, the Data Protection Act 2018, the NHS Data Security and Protection Toolkit (DSPT), and guidance from the National Cyber Security Centre (NCSC).
- Maintaining awareness across our workforce so that all colleagues understand their responsibilities for keeping information safe.
- Requiring our suppliers and partners to meet the same standards of security and compliance.

What You Can Expect from Us

We will:

- Handle personal and sensitive information lawfully, fairly, and transparently.
- Provide secure digital systems and services to support patient care and business operations.
- Train our staff in information security and data protection, and refresh this regularly.
- Monitor and improve our security continuously through risk assessments, audits, and incident reviews.
- Respond quickly to security incidents and keep those affected informed where appropriate.

Our Shared Responsibility

Every Elysium colleague plays a role in protecting information. All staff are required to:

- Follow our security policies and standards.
- Complete regular training and awareness activities.
- Protect patient and business information at all times.
- Report incidents, suspicious activity, or concerns immediately.

How We Achieve This

We ensure our commitments are delivered by:

- Applying centrally defined security standards consistently across all sites and services.
- Maintaining oversight through governance committees, audits, and risk management processes.
- Investigating incidents thoroughly and using lessons learned to strengthen our defences.
- Working with trusted partners and suppliers who meet our security and data protection standards.

Oversight and Governance

We ensure that:

- Information security is led by our Information Security Manager and overseen by senior leadership, with accountability to our Chief Information Officer.
- Security is monitored centrally across all sites to provide consistency and assurance.
- Incidents and risks are reviewed regularly, with lessons learned used to strengthen our defences.
- Our governance framework ensures ongoing compliance with legal, regulatory, and contractual requirements.

By protecting information, we protect the people in our care, the colleagues we work with, and the services we provide. Information security is fundamental to patient safety, clinical excellence, and trust.

Approved by: Nick Costa , CEO
Dated: September 2025

Documentation Control

Document Control	Reference Details
Document Title	Cyber & Information Security Policy (Statement)
Document Reference	SEC-INFO-001-PUB
Date of Issue	September 205
Author	Information Security Manager
Owner	Information Security Manager

Version History

Date	Version	Description	Author
16/09/25	0.1	Draft for Consultation and approval	Information Security Manager