Policy and Procedure on Information Governance

Definitions

Information Governance (IG):

IG is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information.

Information Governance Steering Group:

The Group responsible for developing the procedures for IG and generally promoting IG best practice throughout CareTech Group.

Senior Information Risk Owner (SIRO):

The CareTech Group Board member responsible for leading the group IG programme and acting as advocate for Information Risk on the Board.

Caldicott Guardian:

The senior clinical professional who has a strategic role for the management of Individuals information, including agreeing and reviewing protocols governing the protection, use and disclosure of Individuals information.

The Health and Social Care Network Connection Agreement (HSCN):

The process by which organisations enter into an agreement with NHS Digital so that it can send or receive data across the Health and Social Care Network.

Data Security and Protection Toolkit (DSPT):

The Data Security and Protection Toolkit is an online assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance annually that they are practicing good data security and that personal information is handled securely.

Legislation

Please refer to the Appendix 2 document provided.

Introduction

This policy covers all information systems purchased, developed and managed by, or on behalf of, the organisation and any individual directly employed or otherwise by the organisation.

This policy has been approved by and applies to CareTech Group and its direct and indirect subsidiaries and references to the "CareTech Group" shall be construed as referring to all such companies.

All Employees, irrespective of their role within the organisation, are held by the contents of this policy and are required to follow and uphold the values, principals and expected behaviours of the Company when carrying out their duties and responsibilities.

Purpose

To ensure that CareTech has in place a comprehensive, auditable policy in the manner in which it acquires, processes, stores, shares and disposes of information assets for which it is responsible.

Information is a vital asset, both in terms of the clinical/educational management of individuals and the efficient management of services and resources. Information governance plays a key part in supporting clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

CareTech believes that accurate, timely and relevant information is essential to deliver the highest quality health care and education services. As such it is the responsibility of all clinicians, teachers and managers to ensure and promote the quality of information and to actively use information in decision making processes.

Specific areas within Information Governance are covered in more detail by the Policies and Procedures detailed in Appendix 2.

Scope

For the purposes of this and related policies Information is defined as – data that can be stored in any format, e.g., Paper, electronic, audio or visual, or can be passed by word of mouth.

This policy covers all aspects and types of information within the organisation including:

Individual's Information.

Personnel Information.

Organisation Information.

Structured record systems: paper and electronic.

Unstructured information: paper and electronic.

Transmission of information: fax, email, post and telephone.

Procedures

Scope of Information Governance

Personal Information Governance is a framework to enable CareTech to handle personal and corporate information legally, securely, efficiently and effectively, to deliver the best possible care. It is formed of the following initiatives:

Information Security & Risk Management.

Data Protection and Confidentiality.

Information Lifecycle (including Records Management).

CareTech recognises the need for an appropriate balance between openness and confidentiality in the management and use of information

CareTech fully supports the principles of corporate governance and recognizes its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about individuals and employees and commercially sensitive information.

CareTech also recognises the need to share Individuals' information with other health/education organisations and other agencies in a controlled manner consistent with the interests of the Individual and, in some circumstances, legal compulsion and the public interest.

CareTech will develop and maintain a communications strategy to ensure that individuals (and relatives) are aware of the need for CareTech to hold their personal information, the processes which CareTech use, and the rights they hold as data subjects and Individuals.

CareTech undertakes to maintain high standards of information handling by reference to the HORUS model, where information is:

Held securely and confidentiality.

Obtained fairly and efficiently.

Recorded accurately and reliably

Used effectively and ethically.

Shared appropriately and lawfully.

In order to do this, CareTech abide by the following principles:

CareTech seeks to protect its computer systems from misuse and to minimize the impact of service breaks through general compliance with the requirements of ISO27001 and the development procedures to manage and enforce this. The details of this can be found in policy document 'Information Security Policy'.

CareTech will ensure that all information recorded by CareTech is accurate, complete and available appropriately.

CareTech will use all appropriate and necessary means to ensure that it complies with the Data Protection Act (2018), the General Data Protection Regulations (GDPR) and associated Codes of Practice issued by the Information Commissioner's Office. The details of this can be found in policy document 'Data Protection & Confidentiality Policy'.

CareTech will obtain and share information in compliance with the common law of confidentiality and the Data Protection Act. The details of this can be found in policy document 'Data Protection & Confidentiality Policy' and the associated Confidentiality Code of Practice.

Although not a public authority as defined in the FOIA, CareTech will use all appropriate and necessary means to ensure that insofar as it is required to, it complies with the Freedom of Information Act (2000) and associated Codes of Practice. In practice, this means that CareTech Group will comply with any contractual requirements regarding the Freedom of Information Act (FOIA) and as a general rule will refer any FOIA request back to the public body who commissioned the services.

CareTech will have a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal, as per 'Policy and Procedure on Record Management'.

Year on Year Improvement Plan and Assessment

A self-assessment of compliance with the requirements of the Data Security and Protection Toolkit and Cyber Essentials accreditation will be undertaken each year by the Information Governance Steering Group.

In response to the above assessment CareTech will formulate an Information Governance Improvement Plan each year which will detail the action plans that have been raised through the Toolkit.

CareTech will undertake audits of compliance with the policies and procedures relating to Information Governance on a regular basis.

Awareness and Training

All employees will carry out as part of their induction, and then annually thereafter, Information Governance awareness training via the current group E-learning Web Portal. All staff are to complete the assessment tool.

Top-up or role-based training will be given, or organised, where necessary and at least every 2 years; this can be requested by an individual wanting personal development or arranged at the discretion of a line manager. Contact should be made with a member of the Information Governance Steering Group with regard to this.

CareTech will undertake to ensure the 'Initiative Leads' are given the appropriate training necessary to fulfil their role.

CareTech will also take steps to ensure that there is the appropriate level of awareness within the organisation and arrange awareness campaigns.

Accountability

The management of Information Governance across the organisation will be coordinated by the Information Governance Steering Group, the Terms of Reference for which are included in Appendix 2.

The Director having responsibility for Information Governance is the Senior Information Risk Owner. The supporting organisational structure is provided in Appendix 3.

The diversity of subjects covered requires the identification of a `lead` for each initiative. `Initiative Leads` will be the local expert in the particular subject. The posts designated as Leads are given in Appendix 3.

The Information Governance Steering Group's role is to:

Ensure a coordinated approach to Information Governance across the CareTech Group;

Identify best practice, define and deliver improvement plans;

Work closely with employees across the organisation to ensure that Information Governance standards are understood and adhered to.

Heads of Establishment within CareTech have been designated as Data Protection Champion for their establishment and are responsible for ensuring that the policy and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Standard Forms, Letters and Relevant Documents

Appendix 1 – Related Policies and Procedures

Appendix 2 – Information Governance Steering Group Terms of Reference

Appendix 3 – Information Governance Steering Group Structure

Monitoring and Review

CareTech will undertake a formal periodic review of this policy if there are any changes to procedure, legislation or regulations or best practice guidelines as required.

Revision History

Review Date January 2026

Release Date: January 2023

Signed *Russell Edge*

Russell Edge Senior Information Risk Owner (SIRO) & Data Protection Officer January 2026

This policy must be read in conjunction with the following policies:

CareTech Data Governance Strategy

Appendix 1 CareTech Data Governance Roadmap

Information Security

Risk Management

Records Management

Information Systems Acceptable Use

Access to Records

Confidentiality Code of Practice

Processing of Special Category Data and Criminal Offence Data

Remote Working Policy

Data Protection Impact Assessments