

Information Governance Under the General Data Protection Regulation and NHS Records Management Code of Practice Policy

Introduction

Cornwallis Care Service's information governance policy, which is set out here, has developed in line with the following.

1. All organisations and businesses must comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
2. NHS organisations and those that provide services commissioned by it should follow the *NHS Records Management Code of Practice*.
3. The Information Commissioner's Office is responsible for the implementation of the Data Protection Act 2018, the GDPR and for investigating breaches of data security.
4. NHS commissioners could seek to ensure that its contractors are applying the *NHS Records Management Code of Practice* in its information governance.
5. The Care Quality Commission will ensure that care providers information governance and record keeping complies with the relevant sections of Regulation 17 "Good Governance" of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

Definitions

Information governance represents the systems, policies, procedures and processes adopted by the care service to ensure that data is always:

- obtained fairly and lawfully
- held securely and confidentially
- recorded accurately and reliably
- used effectively and ethically
- shared and disclosed appropriately and lawfully
- disposed of safely to the standards required, when no longer needed.

The policy describes how CCSL manages any data, which it keeps and to which it has access, so that the information is always held safely and securely, and is lawfully used. In carrying on its business of providing care and treatment, the care service will obtain and use the personal data

of different groups of people: the people who use its services and others relevant to them, its employees and others, such as contractors and suppliers of goods and services. CCSL is bound by law and its registration requirements to achieve established standards in its handling and management of information.

In addition to the record-keeping policies described above, the information governance framework includes several interrelated policies and procedures that contribute to its effectiveness. They include:

- access to employees' data
- Caldicott principles
- computer systems and internet: acceptable use
- internet use: staff
- internet use: people receiving care
- IT disposal
- the use of mobile telephones
- quality assurance: monitoring and reviewing the service provision
- sharing information with other providers
- social media.

Legal Requirements

CCSL recognises that information governance requirements have developed from a raft of legislation and statutory guidance, including:

- Data Protection Act 2018 and the GDPR
- the Common Law duty of confidentiality as applied, for example, in the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Freedom of Information Act 2000
- Human Rights Act 1998
- the Caldicott Report and Principles (and their application under the Office of the National Data Guardian)
- Health and Social Care Act 2008 (and regulations)

- Health and Social Care Act 2012
- *Records Management Code of Practice* (applies to NHS and related health and care services, last updated August 2023.)

It also acknowledges the importance of complying with Regulation 17: Good Governance of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which requires registered care providers to have effective systems and processes for, among other aspects of administration, keeping records on every individual, maintaining records and striving for continuous improvements to their systems (see Regulations 17(c), (d) and (f)).

The Information Governance Framework

C CSL recognises that where it is contracted to provide services on behalf of the NHS it should comply with the *Records Management Code of Practice*. This applies particularly where an adult social care provider's care records are integrated and used with individuals' NHS records.

C CSL also recognises that the *Records Management Code of Practice* provides a framework for establishing good information governance practice generally and it will comply with the standards that it sets.

Scope

The information governance framework for this care service covers all records used for or with the care and treatment of the people who use its services, staff records and administrative records likely to contain confidential information. All such records will be handled and kept safely, securely and lawfully to the same standards regardless of their formats, including written records, forms, photographs, audio-visual, CCTV records, computer and smart device electronic records.

The component parts

C CSL recognises that it must achieve agreed standards for each aspect of its information governance system, which, following the GDPR requirements and the *Records Management Code of Practice* require attention to the following.

Records system design

Each set of records and record keeping arrangements are designed so that they are always fit for purpose (including using an appropriate format) and can be correctly handled and maintained. All features of the record keeping arrangements are kept under constant review, regularly audited and changed or replaced if they become unfit for purpose and fail to achieve the required standards.

Records handling and use

CCSL has put into place effective procedures to ensure that records storage, arrangements for authorised access, information sharing, transfer of records, and quality of recording are all maintained.

Audit, review and retention

All records and record-keeping systems are regularly audited and reviewed for their current purpose and quality in line with the care service's auditing schedules. Records that are no longer needed will be stored or archived safely and securely for the recommended or required retention periods, which for NHS providers and commissioners are set out in the *Records Management Code of Practice*.

Appraisal

At the minimum retention date, records will be appraised to identify if they will be required further, and if not, they will be safely disposed of. Where people who use services' health and social care records have been, CCSL will comply with the eight-year retention period stated in Appendix 2 of the *Records Management Code of Practice 2023*.

CCSL recognises that the eight-year retention period given in the *Records Management Code of Practice* is at variance with the three-year minimum retention period that for data protection reasons has applied to care homes where they have record-keeping systems that are independent of NHS systems.

CCSL will safely dispose of all records for which it is responsible that have passed their minimum retention period and are no longer needed. The methods of safe disposal will depend on the type of record. Paper records will always be confidentially shredded, and records kept of the means and date. Electronic records stored on computers, smartphones or other such devices will be disposed of using approved methods and IT expertise.

Management Responsibilities

The service has designated people for information governance in each of its locations and at organisational level. This includes the designation of people to be responsible for the co-ordination and completion of any system auditing and reviewing.

Where responsibilities are delegated to someone other than the registered manager, the person(s) will be responsible to the registered manager, who will be responsible to the registered provider.

Every person with information governance responsibilities has clearly defined roles for ensuring the safe, secure and lawful use of the records for which they are responsible, for oversight of

any or all stages of the lifecycle of the salient records from design to disposal (see above), and for maintaining standards.

Anyone with information governance responsibilities will be suitably inducted and trained to fulfil the requirements of their role and will be required to make regular reports to their line manager so that there is a clearly defined reporting process operating throughout and to the top of the organisation.

Achieving, Maintaining and Improving Information Governance Standards

The care service is committed to ensuring that all personal data that it creates, uses, handles and manages, achieves and maintains the highest standards of information governance possible. It recognises that the current benchmarks are provided by the Information Commissioners Office in its enforcement of the GDPR and the NHS *Records Management Code of Practice*.

The care service considers that it is good practice to benchmark their information governance against these standards and to make any improvements indicated.

The care service considers that it will achieve the recommended standards by, for example:

- having designated staff, who are suitably trained in the role, to be information governance leads for their respective record management duties
- having an information governance management framework based on this policy that covers all aspects of information governance
- ensuring that all care, nursing, non-care staff and contractors supplying goods and services understand how to keep confidential any personal information they receive, and in line with data protection requirements
- ensuring that staff receive suitable training from induction onwards in the care service's policies and procedures for safe handling and using information
- ensuring that all related policies and procedures on record keeping, confidentiality, consent and data protection are always adhered to by all staff, partners and stakeholders
- ensuring that all personal data in any form is kept safe and secure through the issuing of privacy notices
- stating its commitment to continuously improving its information governance through its improvement plan.

Losses and Breaches of Information Safety and Security

The care service will act quickly to repair and mitigate any damage or harm caused by accidental or deliberate loss of sensitive data or breaches of the established policies and procedures in the handling of the data, especially if the events are harmful or potentially harmful to the people who use its services.

The care service will always investigate thoroughly any loss of information or breaches in the handling of sensitive information and will fully co-operate with other organisations that might be involved in the loss or damage, including police if there is evidence that criminal acts have been committed.

Employees who fail in their duty of care to protect sensitive information will be subject to the service's disciplinary proceedings. If the service receives a complaint about the mishandling or loss of personal data, it will investigate the matter through its complaints procedures, which might also entail working with other organisations with whom the data is shared.

The care service will also take suitable action against any third parties with access to sensitive information, who have not followed the required policies and procedures over confidentiality, etc.

In the event of individuals suffering significant harm from any personal data losses or being placed at high risk of being harmed, the service in line with its legal obligations under the GDPR inform the Information Commissioner's Office so that it can investigate.

Related Policies

The policy should be used with other relevant policies on:

- Applications for Access to a Deceased Individual's Care Records
- Confidentiality of Information
- Data Protection and Compliance with General Data Protection Regulation
- Records and Record Keeping -

Individuals' Authorised Access to Records Training

New care staff are trained in CCSLs policies and procedures for record keeping, consent and confidentiality, etc as part of their induction training, which follows the Care Certificate Standards framework.

All staff can expect to receive instruction and dedicated training as needed in the service's record keeping policies and procedures.

Staff with specific roles and responsibilities for information governance at any level in the organisation can expect to receive the relevant training to achieve required information governance standards, and to implement the GDPR and *NHS Records Management Code of Practice*.

Review

Signed: Nicola Hemsley, Operations Director

Policy review date: October 2025

Nex Review Date: October 2027