University Hospital Southampton NHS Foundation Trust

Wessex SDE Data Retention Policy, V1

Trust reference	SDE_POL_006	Version number	1
Description	The Data Retention Policy defines how the Wessex SDE manages, reviews, and securely disposes of all data types in compliance with legal, regulatory, and NHS-specific requirements, ensuring data is only kept for as long as necessary.		
Level and type of document			
Target audience	The audience for the Data Retention Policy includes all staff, contractors, and third parties who create, manage, access, or store organisational data, including Information Asset Owners, the Data Protection Officer, IT personnel, and departmental managers.		
List related documents/policies (do not include those listed as appendices)	SDE_SOP_005: SDE Data Retention and Disposal SOP		
Author(s) (names and job titles)	Wessex SDE Director of Operations, Mark Heffernan		
Policy sponsor	Wessex SDE SRO, Chris Kipps		

This is a controlled document. Whilst this document may be printed, the electronic version posted on Florence is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from Florence.

1. Version control

Date	Author(s)	Version created		Approval committee	Date of approval	Date next review due	Key changes made to document
1/12/25	Mark Heffernan	1		Mikayala King Jo Musgrove	1/12/25	1/12/26	First version with comments from MK, JM and MH

University Hospital Southampton
NHS Foundation Trust

Wessex SDE Data Retention Policy, V1

2. Index

University Hospital Southampton NHS Foundation Trust

Wessex SDE Data Retention Policy, V1

3. Introduction

The mission of the Wessex Secure Data Environment (SDE) (part of a National SDE initiative by NHS England) is to build an online platform where large amounts of NHS patient data can be securely stored, linked together, and accessed by researchers. It has been built to the highest privacy and security standards for NHS data. The service supports the discovery of new and better treatments and medicines, and planning to improve the way the NHS works.

For more information see https://wessexsde.nhs.uk/ and https://digital.nhs.uk/data-and-information/research-powered-by-data/sde-network

4. Scope and purpose

The purpose of this policy is to ensure all organisational data is kept only as long as needed and securely disposed of in line with legal and regulatory obligations. This includes clinical, operational, personal, corporate, and research data without regard to its format or source. It supports compliance with the regulatory framework including the UK GDPR, Data Protection Act 2018, and the Data (Use and Access) Act 2025 (UK DUA). It also aligns with NHS-specific standards such as the Records Management Code of Practice, the Data Security and Protection Toolkit (DSPT), and its underpinning Cyber Assessment Framework (CAF). The policy provides a structured and accountable approach to data lifecycle management supporting transparency, governance, and information rights.

This policy applies to all staff, contractors, and third-party service providers who process, manage, or store data on behalf of the Wessex SDE. It covers all data formats and systems, including physical records, electronic files, databases, email, communications, backups, and archived content across all departments and services. The scope includes data received from partner organisations, e.g. health research data, where the SDE acts as a custodian, processor, or collaborator, ensuring all such data is retained and disposed of in line with legal, contractual, and ethical obligations.

Wessex SDE Data Retention Policy, V1

5. Definitions

Definition	*Description*
Data	Any information held in electronic or physical format, including but not limited to patient records, employee data, emails, financial documents, research datasets, and system logs.
Personal Data	Information relating to an identified or identifiable natural person, as defined under the UK GDPR and Data Protection Act 2018.
Special Category Data	A subset of personal data requiring enhanced protection, such as health information, genetic data, or biometric data.
Data Retention	The practice of keeping data for a defined period to meet legal, regulatory, or operational requirements.
Disposal	The secure and irreversible destruction or deletion of data that is no longer required.
Information Asset Owner	A designated individual responsible for the management, security, and proper handling of specific sets of data within the organisation.
Records Management Code of Practice	NHS guidance that sets out recommended retention schedules and handling practices for health and care records.
DSPT (Data Security and Protection Toolkit)	An NHS assurance framework aligned to the Cyber Assessment Framework (CAF) that requires organisations to demonstrate effective data security and privacy controls.
Data Steward	An individual, team, or external partner responsible for the day-to-day management of a specific data set. This includes ensuring the data is processed, stored, reviewed, and flagged for disposal in line with the retention policy, under the oversight of the Information Asset Owner (IAO). Data Stewards are typically UHS/UoS internal staff but may be external if they have legitimate reason e.g. via contract.

Wessex SDE Data Retention Policy, V1

6. Roles and Responsibilities

Information Asset Owner (IAO):

The Director of Operations (with a designated nominee of SDE IG Functonal Lead) fulfils the role of Information Asset Owner (IAO) and is responsible for:

- Ensuring that all data assets are identified and classified
- Retention periods are defined and applied based on legal and NHS requirements
- The Data Retention Schedule and Disposal Log are appropriately maintained
- Ensuring secure storage, timely review, and appropriate disposal of all data types
- Coordinating with the Clinical Informatics Research Unit (CIRU) to ensure infrastructure and storage services align with this policy
- Liaising with the University of Southampton (UHS) to maintain alignment with corporate governance, assurance, and data protection obligations.

University Hospital Southampton NHS Foundation Trust (UHS):

Provides strategic governance and oversight. Responsibilities include:

- Offering policy alignment, legal interpretation, and risk guidance
- Providing access to Data Protection Officer (DPO) expertise, including support for DPIAs, incident response, and regulatory engagement
- Supporting audits, assurance reporting, and any regulatory submissions
- Ensuring consistency between the organisation's retention practices and those of the wider corporate framework.

Hosting Organisation (CIRU):

Provides the technical infrastructure supporting the organisation's data lifecycle. Responsibilities include:

- Ensuring data storage, access control, and backup systems meet retention and disposal requirements
- Enabling secure deletion and retrieval of data in accordance with the retention schedule and policy
- Supporting Director of Operations in responding to Subject Access Requests (SARs) by providing timely access to relevant data
- Assisting with data breach investigations by supplying system logs, access records, and technical expertise as required
- Communicating any changes to systems or processes that may affect data retention or integrity.

Data Stewards:

- Manage the day-to-day handling and operational control of assigned data types
- Monitor data against retention thresholds and report to IAO
- Support reviews and facilitate secure deletion as per agreed methods
- Document activities to maintain audit trails and ensure compliance.

Wessex SDE Data Retention Policy, V1

Data Sharing Partners:

External organisations that share data with or receive data from the organisation. Responsibilities include:

- Ensuring data sharing agreements specify agreed retention responsibilities, timeframes, and secure disposal methods
- Complying with agreed retention terms and providing assurance on their implementation
- Notifying the Director of Operations of any material changes in data handling that may impact retention or compliance obligations.

7. Retention Principles

Wessex SDE adheres to the following principles for data retention:

1. Necessity

Data is retained only for as long as required to fulfil its intended purpose or to comply with legal, clinical, contractual, or regulatory obligations.
➤ *This includes all data processed within the Secure Data Environment (SDE), including datasets reproduced for secondary use, which must be retained only as long as is justified by their approved project scope and purpose.*

2. Proportionality

Retention periods reflect the sensitivity, criticality, and intended use of the data. Special attention is given to special category data, such as health and biometric data, which may require shorter or more strictly controlled retention.
➤ *Retention policies within the SDE must consider the nature and context of each data instance, especially where copies are generated under approved extraction protocols.*

3. Accountability

Retention decisions are documented and defensible under the UK GDPR, DPA 2018, DSPT-CAF, the Medicines for Human Use (Clinical Trials) Regulations 2004 and its amendments and NHS records policy requirements.
➤ *The Service must demonstrate adherence to retention requirements set by the original data controller and ensure that decisions are traceable and formally recorded.*

4. Security

Data, especially special category and confidential data must be stored securely throughout its lifecycle, with access limited to those with a clear business or clinical need.
➤ *All retained datasets, including secondary copies, must be held within secure SDE infrastructure and subject to access control and audit mechanisms aligned with DSPT-CAF standards.*

Wessex SDE Data Retention Policy, V1

5. Timely Disposal

Once data reaches the end of its approved retention period, it must be reviewed and securely disposed of in a verifiable and auditable manner.
➤ *This applies equally to primary and secondary datasets within the SDE. Disposal methods must be documented, controlled, and subject to review against both organisational policy and the source controller's requirements.*

6. Accessibility

This includes the preservation of electronic data and not just storage. We need to be able to read documents with different file formats during their retention period and preserve metadata alongside too otherwise there is no point in keeping them.

If you can't read it or use it to recreate what you need then there's no point in keeping it in the first place.
➤ *This applies equally to primary and secondary datasets within the SDE.*

8. Retention Periods

Retention periods are determined based on:

- The NHS Records Management Code of Practice for Health and Social Care
- Statutory requirements for example, the UK GDPR, DPA 2018, and UK DUA (2025)
- The Medicines for Human Use (Clinical Trials) Regulations 2004 and its amendments
- Contractual agreements, especially for research or shared data
- Risk-based considerations tied to business, legal, or clinical need.

Special category data, including health, genetic, or biometric information, is subject to enhanced retention controls, including:

- Explicit justification for extended retention
- Additional reviews before archival or disposal
- Restricted access and traceability during the retention period

A comprehensive Data Retention Schedule and Disposal Log are maintained to support operational compliance.

Wessex SDE Data Retention Policy, V1

9. Review and Disposal

All data must be reviewed at the end of its defined retention period to determine whether continued retention is legally justified, operationally required, or should be discontinued. The IAO is responsible for coordinating and documenting the review process across all data categories, with input from relevant Data Stewards and study sponsors.

Disposal of personal or special category data must be irreversible and verifiable. Where data is hosted by the CIRU or retained by a partner, evidence of secure deletion or return must be recorded.

10. Monitoring and Audit

Wessex SDE maintains oversight of data retention and disposal practices through a combination of routine monitoring and formal audit. These activities ensure ongoing compliance with legal, regulatory, and NHS specific requirements, and provide assurance that data is managed consistently and transparently.

Monitoring Responsibilities:

- The Information Asset Owner is responsible for overseeing adherence to the Data Retention Schedule and flagging data approaching its retention threshold.
- Data Stewards are expected to conduct regular checks on datasets under their control to ensure appropriate handling, secure storage, and readiness for disposal as well as maintaining accessibility and preservation during the retention period
- System-level monitoring (e.g. access logs, deletion records) is coordinated with the CIRU to validate data lifecycle activities.

Audit Activities:

An audit plan will be established and reviewed annually. Annual audits will be conducted to verify that:

- Data is being retained and disposed of in line with approved retention periods.
- Disposal actions are fully logged and authorised.
- Exceptions to standard retention practices are properly documented and risk assessed.

Audits may be carried out internally by the Information Asset Owner or designated nominee in collaboration with the UHS, especially where DPO oversight or DSPT compliance reporting is required.

Audit outcomes must be documented, and any non-conformities must trigger remedial action plans with defined owners and deadlines.

Wessex SDE Data Retention Policy, V1

11. Document Review

This policy is subject to regular review to ensure it remains accurate, relevant, and compliant with evolving legal, regulatory, and operational requirements.

The policy will be formally reviewed at least annually by the Information Asset Owner.

Additional reviews will be triggered in response to:

- Changes in legislation or national guidance (e.g. updates to the UK GDPR, DPA 2018, UK DUA 2025, or NHS Records Management Code)
- Organisational changes, such as new systems, data sharing agreements, or hosting arrangements
- Audit findings, incidents, or breaches that reveal gaps or require policy adjustment

Revisions must be documented with version control, including the reason for change and the date of approval.

The UHS may support or approve updates where shared compliance or governance obligations exist.

The most current version of this policy will be accessible to all relevant staff and third parties, and any substantive changes will be communicated accordingly.

Appendices (Stored separately)

Wessex SDE Disposal Log

Wessex SDE Record Retention Schedule

References

https://www.gov.uk/data-protection

SDE_SOP_005: SDE Data Retention SOP