Procedure Group: Information **/** Information and Data Governance
Version no.: 2.2
Date of issue: April 2022
Approved by: IGG

Records Management Procedure

1. Procedure Purpose

Records management is the process by which an organisation manages all aspects of its records, whether internally or externally generated and in any format or media type, from their creation all the way through their lifecycle to their eventual disposal.

St Andrews' records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, and protect the interests of the organisation and the rights of claimants and appellants, staff and members of the public. They support consistency, continuity, efficiency and productivity, and help deliver services in consistent and equitable ways.

St Andrew's Healthcare commits to managing records in line with all legal and professional obligations. We recognise that these may change over time and we will work proactively to identify and fulfil new obligations.

2. Links to Procedure

Users should be aware that the:

- Records Management Procedures
- Data Protection Policy & Procedures
- Information and Data Governance Policy & Procedures
- Information Security Policy & Procedures

All contribute to the Information Governance Framework and that all the Procedures referenced in these directly support our Record Management Procedure.

Policies and procedures available via the Policy A-Z:
Policies - Policies - A-Z (sharepoint.com)

3. Scope

This procedure must be complied with by all staff, volunteers, contractors or others who create, process or access St Andrew's Healthcare Records.

4. Key Requirements

Procedures and operating practices must ensure robust records management which means:

- Records are available when needed;
- Records can be accessed - and that the current version is identified where multiple versions exist;
- Records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- Records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- Records can be maintained through time – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- Records are secure - that access and disclosure are properly controlled;
- Records are retained and disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value;
- Records are owned – key information assets are tracked and there is clear accountability for records.
- Staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management.

The Charity recognises that there are tangible risks associated with record management that can have legal, financial, operational and reputational consequences. The Charity will:

- Implement appropriate governance structures to identify, own and monitor Charity wide information risks
- Implement appropriate procedures to identify information risks in operational activity and projects.
- Identify and implement controls, procedural and technical, to appropriately mitigate the information risks

5. Monitoring and Oversight

The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a yearly basis or sooner if the need arises.

Assurance is to be provided by independent reviews by both Internal and External Audit as appropriate.

This Procedure is formally reviewed and approved by the Information Governance Group (IGG) which reports into the Charity Executive Committee (CEC) and Board.

A failure to comply with the terms of the Procedure and the related Procedures may result in disciplinary action being taken against you, up to and including dismissal from St Andrew's Healthcare. For contractors, third parties or consultants non-compliance may result in termination of your contract.

In addition, a number of data protection laws covers processing of personal data. Breaching these laws can:

- Expose the Charity to legal and financial penalties or other enforcement actions
- Expose you personally to legal or financial penalties where you have acted outside agreed operating practices or negligently.

6. Training

Records are created throughout the Charity and relevant training is provided based on operational role. For example if you will be responsible for clinical records you will be provided appropriate RiO training.

Additionally St Andrew's Healthcare provides and records the following training:

- Information and Data Governance is included in the corporate induction session for all new starters,
- Mandatory e-Learning course which all staff have to complete upon induction and then annually which includes the key topics of this policy,
- The Information Governance Team can also co-ordinate or provide specialist information, advice and guidance relating to this procedure on request.

7. References to Legislation and Best Practice

The technology and legislative environment will continually evolve but we recognise that the Records Management Code of Practice for Health and Social Care 2016 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It is based on current legal requirements and professional best practice and was published on 20 July 2016 by the Information Governance Alliance (IGA).

Not all of the code is relevant to St Andrew's Healthcare, but continues to be an important reference for best practice across the public and private health and social care sector.

8. How to request a change or exception to this procedure

Please refer to either the Policy and Procedure Update Application Link
Or the exception process Policy and Procedure Exception Application Link

9. **Key changes** - please state key changes from the previous version of the procedure

Version Number	Date	Revisions from previous issue
V1.12	Dec 2019	Cosmetic update required to update terminology such as DPA 1998 to DPA 2018, prior to complete refresh of this procedure and associated procedures
		For prior document revision history refer to the v1.12 publication
V2.0		This is the first version of a rewrite of this procedure to fit the current Information Governance Policy Framework.
V2.1	Apr 2022	Data update and author update to DPO
V2.2	June 2023	Extended review date by 12 months