Data Security Protection Toolkit

Information Governance Statement for Health Research v4.1

Document information	
Document name	DSPT Information Governance Statement for Health Research v4.1
Author	By Wendy Craig
Issue date	24/06/2022
Approved by	FMS IGHR
Next review	June 2023

Document history		
Version	**Date**	**Summary of change**
V0.1	04/10/2016	Reference to IGT Staff Handbook added.
V0.3	17/10/2016	Adding front page, addition of Document Reference,
V1.0	31/10/2016	Approved by TG as amended by FMS IGSG
V2.0	28/04/2017	References added to University ISMF
V2.0	28/04/2017	Links to other supporting material added.
V3.0	29/05/2018	Reference to IGT changed to DSPT
V3.0	10/12/2019	Reviewed updated graphics and version
V4.1	14/01/2022	Add Health Research to Document Title

1. Introduction

Information is a particularly vital asset within clinical research activities and other related patient data analysis activities such as public health planning, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information used within the research and analytics environment is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2. Purpose of the Statement

This Information Governance Statement provides an overview of the universities approach to information governance(IG) for the purpose of submission of the Data Security Protection Toolkit (DSPT). This includes reference to the procedures in use and details about the IG management structures within the Framework. This statement does not replace University policies or procedures around data protection and information security. It is considered to supplement these documents.

3. Our approach to Information Governance

The university undertakes to implement information governance effectively and will ensure the following requirements of DSPT are met where necessary:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Information governance training will be available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4. Procedures

Information Governance requires implementation of the following procedures underpinned by the following procedures:

- **Joiners and leavers procedure** that sets out procedures for the management of access to computer-based information systems. This is detailed in the DSPT Handbook;
- **Confidentiality Audit Procedure** that sets out procedures around the transfer of confidential information. Copy available here.
- **Incident management procedure** that sets out the procedures for managing and reporting information incidents. This is detailed in the DSPT Handbook;

5. Guidance for staff

The DSPT Handbook sets out the procedures to ensure staff compliance with the requirements for DSPT. This covers the following areas:

- **Confidentiality:** sets out the required standards to maintain the confidentiality of personal information; obligations around the disclosure of information and appropriately obtaining patient consent;
- **Access control:** guidelines on the appropriate use of computer systems;

- **Information handling:** guidelines on the secure use of patient information;
- **Secure Transfer of Personal and Sensitive Information;** sets out the ways in which the transfer of personal and sensitive information would be permissible.
- **Using mobile computing devices:** procedures on maintaining confidentiality and security when working with portable or removable computer equipment.
- **Information incidents:** guidelines on identifying and reporting information incidents.

6. Responsibilities and accountabilities

The designated Information Governance Lead for the Information Governance Framework is the Information Governance Officer (FMS).

The key responsibilities of the lead are:

- Ensure there is an up to date IG Statement is in place and that it is reviewed annually by FMS IGHR
- Ensure that the FMS DSPT IG Framework which is the approach to information handling for DSPT is communicated to all staff and made available to the public
- Receive all necessary and reasonable assurances from staff given information governance assurance, information security assurance and data protection and confidentiality assurance responsibilities
- Receive assurances in particular for the DSPT monitoring of information handling activities to ensure compliance with law and guidance
- Evaluation and analysis of the effectiveness of the Information Governance Framework based on results of measurement and monitoring
- Recommend and support when appropriate regular Information Governance management reports to the FMS IGHR
- Receive assurances that FMS has submitted the FMS IGHR approved annual Data Security Protection Toolkit Assessment
- Receive assurances that all toolkit members are sufficiently trained to support their role.
- Be appraised of monitoring visits from appropriate bodies, (e.g. regulatory visits) and to delegate all necessary and reasonable support through the Information Security Officer and other staff who have Information Security Assurance and Data Protection and Confidentiality Assurance responsibilities

The **senior management (director, team leader, research fellow, etc)** who are named on the Toolkit are responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework.

All **Toolkit members**, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy statement and the procedures and guidelines produced to support it.

7. Approval

This policy statement has been approved by the FMS IGHR and will be reviewed annually.