Data Security Protection Toolkit Confidentiality Audit Process

Document Information	
Document Name	Toolkit Confidentiality Audit Process
Version	3
Issue Date	24/06/2022
Approved By	FMS IGHR
Next Review	30 June 2023

Document History		
Version	**Date**	**Summary of change**
V1	09/09/2016	Initial Document
V1.1	31/10/2016	Rephrasing of 5.1
V2	09/04/2018	Updated to include reference to GDPR
V2	09/04/2018	Reference to University Policy and Guidance
V3	22/01/2020	Removed references to items no longer supported.
V3	22/01/2020	New section on timings of audits.
V3.1	30/04/2021	Update documents to refer to FMS IGHR

1.0 Introduction

1.1 This procedure establishes appropriate confidentiality audit procedures to monitor access to personal identifiable data throughout FMS. This work forms part of the FMSs Information Governance Toolkit framework and meets requirements within:

- the NHS Information Governance Toolkit
- the NHS Confidentiality Code of Conduct
- the NHS Care Record Guarantee
- Data Protection Act 2018
- EU General Data Protection Regulation
- UK General Data Protection Regulation
- Regulation of Investigatory Powers Act (RIPA) 2000
- Human Rights Act 1998

2.0 Scope of the Audits

2.1 All work areas within the toolkit which handles Personal Identifiable Data (PID) will be subject to the confidentiality audit procedures.

2.2 Access to electronic and manual personal identifiable data will be audited. Audits across all sites referenced within the toolkit will be undertaken and this will capture any inconsistencies in practices.

2.3 A each project will be audited over the course of the project.

3.0 Audit Approach

3.1 The Audits will review compliance in the following topic areas, where applicable, to establish evidence:

- Staff awareness of the toolkit policies and guidelines concerning confidentiality
- Appropriate recording of consent, and appropriate ethics
- Appropriate allocation of access rights to systems
- Appropriate staff access to physical areas
- Secure storage of and appropriate access to filed hard copy person-identifiable notes and information
- Appropriate use and security of the telephone in open areas
- Storage of personal identifiable data (PID) in public areas

3.2.1 The Auditor will follow audit procedures and provide the following deliverables:

- Planned and implemented audit programme
- A spreadsheet or database to record audit findings and outcomes
- Audit reports and recommendations for the FMS Information Governance for Health Research (FMS IGHR)
- Support for action plans to address any areas requiring review
- Reports to the Toolkit Information Risk Owner (TIRO) concerning any identified breaches.

3.3 Audit methods and facilities to be utilised:

- Notified audit visits with structured templates
- Spot checks, with structured templates, to random work areas to confirm PID is used and obtained fairly and lawfully
- Investigation of reports on the FMS IGHR standing agenda for Serious Untoward Incidents

(SUIs).

3.4 The IG Lead will arrange an audit programme annually.

3.5 Audit results will be collected on a standard template and then held for future reporting and analysis.

4.0 Audit Findings

4.1 Results from the audits will be collected in a standard template and then recorded in a spreadsheet or database for future reporting and analysis. The report will be submitted to the Information Governance for Health Research group and will highlight any areas requiring further development and make recommendations concerning any corrective actions
required.

5.0 Newcastle University Disciplinary Policy and Procedures

5.1 In the event that there has been an incident of gross misconduct the Disciplinary Procedure will be invoked.

5.2 The University is committed to the avoidance of formal disciplinary procedures wherever possible by addressing problems as soon as they arise.

Appendix 1 – Glossary

FMS IGHR: Information Governance for Health Research group. This group is responsible to the FMS
Senior Executive Group (SEG) for the maintenance of the DSPT information governance framework
for FMS. It is responsible for ensuring that the Data Security Protection Toolkit Support is available to the University Research Community.

Personal identifiable Data (PID): is defined as any information about a person which would allow that person to be identified. Any inappropriate disclosure of that personal identifiable data would breach their right to privacy, or present a risk of identity theft.

RIPA: Regulation of Investigatory Powers Act 2000. The Act regulates the powers of public bodies to carry out surveillance and investigation, including the interception of communications.

FMS: Faculty of Medical Sciences

SUI: Serious Untoward Incident, NHS terminology to describe incidents that would have a negative impact to an organisation.

Appendix 2 – Monitoring Questions

Project Members

1. **Have all members completed the relevant training in accordance with the training matrix.**
2. **Have all project members agreed to the terms of the DSPT.**
3. **Do project members know where to find up to date documentation.**

Equipment

1. **Do all project computers have up to date antivirus installed?**
2. **Are they encrypted?**
3. **Do they have DA configured?**

Data storage

1. **Do only registered users have access to the required Information assets?**
2. **Have the Joiners and Leavers process been followed?**
3. **How has the Data been accessed whilst working from home?**
4. **Is data stored where it's supposed to?**
5. **Is data backed up?**

Processes

1. **Has the project DPIA been completed and has it been reviewed?**