TFR Pharma

PembrokeCastle PHARMACY MENDUSPHARMACY

Information Governance – IT Security Policy			Version 1.0
Statement Prepared by:	Statement Approved by:	Date Next Review Due:	1/3/26
Mark Roberts	Nathan Raymond		
Date Version Prepared:	Date Version Approved:	Date Review Takes Place:	
19/2/24	26/2/24		

1.0 Introduction

This Pharmacy Group will use information in many forms e.g. written, spoken or graphical in nature. The information will be transmitted and stored in a variety of ways e.g. on paper, electronically etc. The creation, storage and retrieval of such information are vital to the day to day running of the Pharmacies.

2.0 Purpose

Much of the information the Pharmacy group processes is personal, sensitive and confidential. It is essential that an Information Governance culture is established to enable information to be used and shared between those who need to use it whilst protecting it from unauthorised access or loss. The basic principles that need to be maintained are:

1. **Confidentiality –** The protection of information from unauthorised access;
2. **Integrity –** Safeguarding the accuracy and completeness of information and processes;
3. **Availability –** Ensuring that information is available to authorised people when needed.

3.0 Scope

This policy and supporting procedures apply to all staff, including permanent, temporary, students/trainees, secondees, volunteers and contracted third parties of the Pharmacy group.

This policy and supporting procedures applies to paper records, computerised records, and any other media used to record information within the Pharmacy building or any other premises where the information is being used or processed.

4.0 Aims and Objectives

The aims and objectives of the Information Governance and IT Security Policy, and its supporting procedures, are to ensure that the Pharmacy puts in place an Information Security Management System (ISMS) that:

- Complies with the Data Protection Act 2018 & GDPR;
- Complies with the principles of the Caldicott Report 1997;
- Complies with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004;
- Licenses and registers all commercial software in use within the Pharmacy Group;
- Implements appropriate security controls for all business critical manual and IT recording systems used within the Pharmacy Group;
- Implements appropriate security measures that ensure confidentiality, integrity and availability of information and IT systems;
- Makes staff aware of business continuity planning issues;
- Makes all staff aware of the limits of their authority and their accountability.

5.0 Responsibilities

The Lead for Information Governance and IT (IG & IT) Security, **Nathan Raymond**, fulfils the role of **Data Controller** under the Act, is the responsible Superintendent Pharmacist for the Company, and has overall responsibility for the area of Information Governance and IT Security within the Pharmacy and the implementation of this policy and its supporting procedures.

5.1 The Company has an appointed **Data Protection Officer** – **Mark Roberts**, and fulfils this role under the Act, ensuring appropriate compliance with the Act and obligations under GDPR. The DPO is the central point of contact for advice and guidance on all areas of compliance for Information Governance, responsibilities under the Act and GDPR, working to the rules laid out by the UK Supervising Authority - the Information Commissioners Office.

5.2 The **Data Controller** has the following responsibilities:

- **Caldicott Guardian Lead** and will have specific responsibility for ensuring the Pharmacy group operates within the Caldicott Principles that apply to patient identifiable information;

- **Security Manager** with specific responsibilities for ensuring the physical security of the Pharmacy group. This includes the security and access controls for the Pharmacy IT systems, and the security of all information the Pharmacy group holds;

- **System Manager** with the day to day management responsibilities for the Pharmacy IT systems.

All company staff will be responsible for ensuring that they remain aware of the requirements incumbent upon them for them to ensure compliance on a day to day basis. This includes maintaining confidentiality and secure storage of information and being aware of situations where disclosure may or may not be required.

6.0 Policy Implementation and Monitoring

This policy will be delivered and maintained by the implementation of a framework of security procedures.

All staff will be made aware of the policy and supporting procedures. Breach of this policy may lead to disciplinary action being taken. Depending on the circumstances this could range from remedial training to dismissal.

Monitoring compliance with this policy will be achieved by undertaking regular audits.

This policy will be reviewed annually and as and when there are any legislative changes affecting Information Governance and IT Security.

7.0 References

Supporting Policies, Procedures and Guidelines

- Records Management Policy
- Data Protection, Confidentiality and Subject Access Procedure

- Freedom of Information Act and Environmental Information Regulations Procedure
- Incident Reporting Procedure
- Safe Haven Guidance
- Removal, Storage and Transportation of Patient Identifiable Information Guidance
- Anti Virus Procedure
- System Access Procedure
- System Backup Procedure
- Disposal of IT Equipment and Media Procedure
- Business Continuity Plan

8.0 Legislation and Guidance

- The Data Protection Act 2018
- The General Data Protection Regulations
- The Caldicott Report 1997
- The Human Rights Act 1998
- Computer Misuse Act 1998
- The Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Copyright Design and Patent Act 1998
- The NHS Baseline IT Security Standards
- Standard for Information Security ISO27001 & ISO17799
- DH Records Management: NHS Code of Practice
- The Information Commissioners Office