CATHAYS SURGERY

I.T. & SECURITY POLICY

Version: 1
Last Updated: August 2021

Information Security Policy

CATHAYS SURGERY

Contents

Information Security Policy

CATHAYS SURGERY

1.0 Introduction

A General Medical Practice 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 or on film, commonly called "information assets". The creation, storage, and retrieval of such information is vital to the day to day running of the Practice.
Much of the information the Practice needs is personal and confidential. The purpose of Information and I.T. Security is 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 of information security that need to be maintained are:

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

2.0 Scope

The Practice policy for Information and I.T. Security applies to all persons that access Practice information. This includes all members of staff, students/trainees, secondees, volunteers and contracted third parties (including agency staff) of the Practice.

The policy applies to paper records, computerised records, and any other media used to record information within the Practice building, any branch surgery, or any other premise where the information is being used or processed.

Failure to comply with the policy may result in disciplinary action or even prosecution.

3.0 Policy Objectives

The objectives of the Information and I.T. Security Policy are to ensure that the Practice: -

- Complies with the Data Protection Act 2018
- Complies with the principles of the Caldicott Report 1997
- Complies with the Freedom of Information Act 2000
- Complies with the Environmental Information Regulations 2004
- Licenses and registers all commercial software in use within the Practice
- Implements appropriate security controls for all business-critical manual and I.T. recording systems used within the Practice
- Implements appropriate security measures that ensure the confidentiality, integrity and availability of information and I.T. systems
- Makes staff aware of business continuity planning issues
- Makes all staff aware of the limits of their authority and their accountability
- Ensures that staff are aware of the Computer Misuse Act (1990)

4.0 Responsibilities

The Practice Manager is responsible for ensuring the highest level of commitment to the policy and the availability of resources to support its implementation and associated legal requirements

The Practice Manager is responsible for the implementation of this policy throughout the practice, and in addition, they must ensure that all staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training.

The Practice's staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Breaches of the policy must be reported in line with the practice's reporting processes and dealt with in line with the practice's disciplinary process where appropriate.

It is also the responsibility of the Practice Manager to make sure that the Practice has the following posts in the management structure, or that the duties of the post holders are incorporated into the roles and responsibilities of specific senior posts:

Data Protection Officer

Your Practice is required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters.

Caldicott Guardian

Member of Staff with specific responsibility for ensuring the Practice operates within the Caldicott Principles that apply to Patient Identifiable Data;

Senior Manager

Senior Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters

4.1 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance.

Failure to do so may result in disciplinary action.

All staff should undertake their mandatory, annual, Information Governance training and understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected beach of information security within the organisation. Their responsibility for raising any information security concerns with the Head of Corporate ICT Technology & and Security.
- Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

5.0 Policy Framework

5.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions and descriptions.

5.2 Security Control Assets

All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

In the event of loss or theft of an electronic portable device, the incident must be reported to the Practice Manager and an incident report undertaken.

Users must not install any software on the mobile working devices without prior authorisation and assessment by the Practice Manager and the ICT provider.

5.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the Practice Manager.

5.4 Computer Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
Authorisation to use an application shall depend on the availability of a license from the supplier.

5.5 Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
Authorisation to use an application shall depend on the availability of a license from the supplier.

5.6 Equipment Security

In order to minimise loss of, or damage to, all assets, all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards by the Practice Manager.

5.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of NHS England.

5.8 Information Security Events and Weaknesses

All Cathays Surgery information security events, near misses, and suspected weaknesses are to be reported to the Data Protection Officer Service (NWISGMPDPO@wales.nhs.uk) and where appropriate reported as an Adverse Incident to the ICO within 72 hours of discovering the breach.

5.9 Classification of Sensitive Information

The Practice Manager shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance.

5.10 Protection from Malicious Software

Users shall not install software on the organisation's property without permission from the Practice Manager.
Users should be informed that breaching this requirement may be subject to disciplinary action.

5.11 Removable Media

Removable media that contain software require the approval of the ICT Senior Manager or Head of ICT Technology & and Security before they may be used on NHS Wales systems.

Users breaching this requirement may be subject to disciplinary action.

5.12 Protection from Malicious Software

The organisation and its ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software.
All staff shall be expected to co-operate fully with this policy.
Users shall not install software on the organisation's property without permission from the Practice Manager and check with Primary Care Service Desk.
Users breaching this requirement may be subject to disciplinary action.

5.13 Removable Media

Corporate IT systems automatically encrypt removable media. Removable media that contain software require the approval of the from the Practice Manager.
Users breaching this requirement may be subject to disciplinary action.

5.14 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. NHS Wales will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.
The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

5.15 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by Primary Care Service Desk & and Security. Your IT Manger (if in post) and Practice Manager.

5.16 Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).
Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

5.17 Training & Awareness

Data Security and Protection training is mandatory, and all staff are required to complete annual on-line Information Governance and Confidentiality training.

5.18 IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure must be complied with when:
A new process is to be established that involves processing of personal data (data relating to individuals).
Changes are to be made to an existing process that involves the processing of personal data;

- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data.
- Introducing any new technology that uses or processes personal data in any way

6 Distribution and Implementation

6.1 Distribution Plan

This document will be made available to all Staff via the Cathays Surgery internet site.
A global notice will be sent to all Staff notifying them of the release of this document.
A link to this document will be provided from the Cathays Surgery intranet site.

6.2 Training Plan

A training needs analysis will be undertaken with Staff affected by this document. Based on the findings of that analysis appropriate training will be provided to Staff as necessary.

6.3 Monitoring Training Compliance

Monitoring Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Team, together with independent reviews by both Internal and External Audit on a periodic basis. The Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

7.0 Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology;
- Change in Senior personnel e.g. Practice Manager or Senior Partner or;
- Changing methodology.

8.0 Equality Impact Assessment

This policy has been subject to an equality assessment.
The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.
As part of its development this document and its impact on equality has been analysed and no detriment identified.