# Policy 10 - Data Security & Protection

## Introduction

The Data Protection Act 1998 (DPA) requires a clear direction on Policy for the security of information within the Practice.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

The following is a Statement of Policy which will apply:

## The Policy

* The Practice is committed to security of patient and staff records.
* The Practice will display a poster in the waiting room, explaining the practice policy to patients.
* The Practice will make available a leaflet on Access to Health Records and Data Protection for information for patients.
* The Practice will take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient’s consent, unless otherwise legally compliant.
  + This will include training on Confidentiality issues, DPA principles, working security procedures, and the application of Best Practice in the workplace.
* The Practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
* The Practice will maintain a system of “Significant Event Reporting” through a no-blame culture to capture and address incidents which threaten compliance.
* DPA issues will form part of the Practice general procedures for the Management of Risk.
* Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

**Signed**:

**Caldicott Guardian** ………………………………………**Date**: 23rd March 2021

**Practice Manager**…………………………………………**Date**: 23rd March 2021

# Data Protection Act – Patient Information

We need to hold personal information about you on our Computer system and in paper records to help us to look after your health needs.

***Please help to keep your record up to date by informing us of any changes to your circumstances.***

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. Your doctor is responsible for their accuracy and safe-keeping.

From time to time, it may be necessary to share information with others involved in your care. We will always ask for your consent if we need to discuss your records or care with staff from another caring organisation. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you.

Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details and our patient information leaflet. An appointment will be required. In some circumstances a fee may be payable.

# Computer System Security

|  |  |
| --- | --- |
| 1. | Key members of staff have access to ‘Administrator’ rights to the network which allow the addition or removal of computer programs (Practice Manager and IT manager). These rights also give access to the server operating system. |
| 2. | Software installed on specific individual PCs e.g. payroll and accounts packages, can only be accessed/amended by those with administrator rights or individual members of staff who have been given authorization. Such software packages can only be accessed by entry of secure passwords. |
| 3. | The practice clinical software (SystmOne) has built in security features which are controlled by the use of smartcards. These are controlled by the Registration Authority within the CSU and allow us to control individual members of staff access to screens and templates appropriate to their role. |
| 4. | The practice manager/IT Manager has access to add/amend/delete users to the network and request users to be added/amended on the clinical software. |
| 5. | For further information about SystmOne user setup and security access you should refer to S1 built in help files, the practices smartcard policy and also refer to the Registration Authority at the CSU for guidance on smartcards and adding users. |
| 6. | ‘Choose and Book’ features can only be accessed by members of staff issued with appropriate access rights on their smartcard. Training is necessary before using the electronic referral system. |
| 7. | All PCs have internet access. Members of staff should refer to the practice policy and guidelines for Electronic Communication before accessing the internet.  Please speak to the Practice/IT Manager to apply for an NHS e-mail address and access. |
| 8. | All smartcards should be kept securely at all times. They should not be left logged in a computer and left unattended. Please refer to the smartcard policy for further guidance. |

**Policy 10 - Data Security & Protection**

**Document Control**

**A. Confidentiality Notice**

This document and the information contained therein is the property of The Swineshead Medical Group

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from The Swineshead Medical Group.

**B. Document Details**

|  |  |
| --- | --- |
| **Author and Role:** | David Harding, Practice Manager |
| **Organisation:** | The Swineshead Medical Group |
| **Document Reference:** |  |
| **Current Version Number:** | V1 |
| **Current Document Approved By:** | David Harding |
| **Date Approved:** | 3rd February 2020 |

**C. Document Revision and Approval History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Version Created By:** | **Version Approved By:** | **Comments** |
| V1 | 2 Feb 19 | David Harding | Sarah Baxter | Original – V1 |
| V2 | 3 Feb 20 | David Harding | Fiona Anderson | No change from Original |
| V3 | 23 Mar 21 | David Harding | Fiona Anderson | No change |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |