# **Herstmonceux Integrative Health Centre**

# **Data Security Policy V10 last reviewed March 2021**

## Introduction

This Data Security Policy is regarding the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, GDPR 2018, The Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality).

## Purpose

The purpose of this document is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

This Data Security Policy covers:

* + - Physical Access Procedures;
		- Digital Access Procedures;
		- Access Monitoring Procedures;
		- Data Security Audit Procedures;
		- Data Security Breach procedures.

## Scope

This policy includes in its scope all data which we process either in hardcopy or digital copy,

this includes special categories of data.

This policy applies to all staff, including temporary staff and contractors.

## Physical Access Procedures

Physical access to records shall only be granted on a strict ‘Need to Know’ basis.

During induction each staff member, who requires access to confidential information for their job role, will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation.

Our staff must retain personal and confidential data securely in locked storage when not in use and keys should not be left in filing cabinets and doors.

All offices, when left unoccupied, must be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage.

The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

We will risk assess each storage location to ensure that the data is properly secured. This risk assessment forms part of the IAR.

All staff have access to all storage locations

An audit will be completed annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit Procedures [7] below.

## Digital Access Procedures

Access shall be granted using the principle of ‘Least Privilege’. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.

Each user is identified by a unique user ID, and a personal NHS Smartcard, so that all access is auditable.

During induction each staff member, who requires access to digital systems for their job, role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access.

A record is kept, by the IM&T Lead, of all users given access to the system.

Any changes to user access requirements are actioned by the Practice Manager or IM&T Lead.

The IAR will contain the location of all confidential and sensitive personal information which is digitally stored.

We will follow robust password management procedures and ensure that all staff are trained in password management.

As soon as an employee leaves, all their system logons are revoked.

As part of the employee termination process the Practice Manager or IM&T Lead is responsible for the removal of access rights from the computer system.

The Practice Manager or IM&T Leadwill review access rights annually. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.

When not in use all screens will be locked

## Access Monitoring Procedures

The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

Areas considered in the compliance check include whether:

* Allocation of administrator rights is restricted;
	+ - * Access rights are regularly reviewed;
			* Whether there is any evidence of staff sharing their access rights.
			* Staff are appropriately logging out of the system;
			* Our password policy is being followed;
			* Staff understand how to report any security breaches.

## Data Security Audit Procedures

Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme.

Audits will be carried out as required by some or all of these methods:

* Unannounced spot checks to random work areas;
* A series of interviews with management and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by the IM&T Lead

The following checks will be made during data security audits:

* The Information Asset Register has been reviewed, updated and signed off;
* The Record of Processing Activities has been reviewed, updated and signed off;
* Previous confidentiality incidents and actions, including disciplinary, taken;
* Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;
* Appropriate communications with service users;
* Appropriate recording and/or use of consent forms;
* Appropriate allocation of access rights to confidential information, both hardcopy and digital;
* Storage of and access to filed hardcopy service user notes and information;
* Correct process used to securely transfer personal information by post, fax or email
* Appropriate use and security of desk and mobile devices in open areas;
* Security applied to PCs, laptops and mobile electronic devices;
* Evidence of secure waste disposal;
* Appropriate transfer and sharing arrangements are in place;
* Security and arrangements for recording access applied to manual files both live and archive, *e.g.* storage in locked cabinets/locked rooms.

## Data Security Breach Procedures

In order to mitigate the risks of a security breach we will:

Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures;

Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach;

Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place.

In the instance that it appears that a data security breach has taken place:

The staff member who notices the breach, or potential breach, will complete a Data Security Breach Incident Report Form without delay, which will be handed to the Practice Manager or IMT & Lead

The Practice Manager or IMT & Lead will complete the rest of the Incident Report Form and conduct a thorough investigation into the breach;

In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner’s Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk)

As part of our report we will provide the ICO with the following details:

* The nature of the personal data breach (i.e. confidentiality, integrity, availability)
	+ - * The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);
			* The categories and approximate number of personal data records concerned;
			* The name and details of our Practice Manager or IMT & Lead
			* The likely consequences of the breach;
			* A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

The Practice Manager or IMT & Lead will inform, directly and without undue delay, any individual that their personal data has been breached.

A data security breach must be marked on the IAR and will prompt an audit of all processes in order to correct any procedure which led to the breach;

A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

## Responsibilities

The Practice Manager & IM&T Lead hold responsibility for

* + - physical security
		- updating and auditing the IAR and ROPA
		- digital access
		- managing breaches
		- data security audits

|  |  |
| --- | --- |
| **Staff** | **Date audited** |
| Spot check that staff understand their responsibility towards data security |  |
| Spot check that staff are aware of our data protection policies |  |
| Have staff received training on data protection? |  |
| Have any staff undergone disciplinary action in relation to data protection and security? |  |
| Spot check that staff understand how to report security breaches and near misses. |  |
| **Physical Access to hardcopy records** |  |
| Check the record of which staff have access to confidential areas is up to date. |  |
| All offices, files, or cabinets which contain confidential information are kept locked when not in use. |  |
| Has all confidential waste been disposed of securely and are there destruction certificates? (If applicable) |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records? |  |
| **Digital Access to records** |  |
| Is the allocation of administrator rights restricted? |  |
| Have staff access rights been reviewed? |  |
| Check if there is any evidence of staff sharing access rights. |  |
| Screens are locked when not in use. |  |
| Check that our password policy is being followed |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records? |  |
| Have appropriate security measures been applied to all computers, laptops and mobile devices? |  |
| Staff are using computers appropriately e.g. no personal use, no downloading unapproved software, no social media use etc. |  |
| **Sharing data** |  |
| Our procedures for safely sharing personal information via post are being followed. |  |
| Our procedures for safely sharing personal information via fax are being followed. |  |
| Our procedures for safely sharing personal information via secure email are being followed. |  |
| **Legal Checks** |  |
| The Information Asset Register has been reviewed and signed off. |  |
| The Record of Processing Activities has been reviewed and signed off. |  |
| Records of consent are up to date and still applicable. |  |

Appendix: Data Security Audit Checklist