

|  |  |
| --- | --- |
| < Insert name of pharmacy>**Data security and information governance policy** | <Insert pharmacy logo> |
| Doc prepared by: | Doc approved by: | Date next review due: |  |  |
| Date prepared: | Date approved: | Date review takes place: |  |  |

|  |
| --- |
| ***About the use of this document and related resources****: This* [*data security*](http://psnc.org.uk/ds) *document assists the pharmacy’s aligment with the*[*Data Security and Protection Toolkit (DSPTK)*](http://psnc.org.uk/dsptk)*. Related pharmacy policies are at PSNC’s* [*data security templates webpage*](http://psnc.org.uk/dstemplates)*.* |

**Purposes of this policy**

This policy sets out the procedures and management accountability and structures that have been put in place within the pharmacy to safeguard the movement of personal data in the pharmacy.

**Underpinning procedures**

The following procedures ([psnc.org.uk/dstemplates](http://www.psnc.org.uk/dstemplates)) have been put in place to support the confidential handling of information within the pharmacy and the sharing of this information with other organisations:

* **Staff Confidentiality Code of Conduct** (sets out the standards expected of staff in maintaining the confidentiality of patient information including dealing with data being processed in and out of the pharmacy);
* **Staff Access Control and Password management SOP** (sets out procedures for the management of access to computer-based information systems);
* **Data Transfer SOP** (sets out procedures around the secure transfer of data, collecting consent and maintaining confidentiality within the pharmacy including the use of safe havens);
* **Incident management SOP** (sets out the procedures for responding to a security breach);
* **Business Continuity SOP** (sets out the procedures in the event of system failure);
* **Portable Device Staff Guidelines** (provides guidance for staff use on the use of portable devices).
* **Privacy notice** provides patients with information about how you process data.
* **Data Quality policy** (provides guidance and training for staff about good data quality processes)

**Staff duties and responsibilities**

All staff, whether permanent, temporary or contracted are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day-to-day basis. These includes maintaining confidentiality of data, ensuring secure storage of data and being aware of situations where disclosure may be required or may not be required. All staff should also maintain good password practices e.g. separate passwords for separate systems, using three random words etc (see also the ‘Staff Access Control and Password management SOP’).

**Accountability and responsibility for this policy**

The designated Data security and IG lead in the pharmacy is responsible for overseeing day to day data security issues; developing and maintaining policies, standards, procedures and guidance, coordinating data security in the Pharmacy, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

The pharmacy contractor (owner) is responsible for ensuring that sufficient resources are available to support the implementation of data security procedures in order to ensure compliance with legal and professional requirements and the NHS information governance requirements.

**Data protection by design and default**

The pharmacy IG lead(s) or equivalent will support the ‘baking in’ of data protection principles if the pharmacy begins with a new type of data processing. A Data protection impact assessment may be e.g. use of a new patient app to support pharmacy and patient interactions. For some types of new data processing, a DPIA may be required. Pharmacy templates including pharmacy DPIAs are available at: [psnc.org.uk/dstemplates](https://psnc.org.uk/dstemplates).

**The national data opt-out system for patients**

The [national data opt-out system for patients](https://psnc.org.uk/optout) allows patients to directly express their opt-out preference about whether health and care organisations can process their personal identifiable information where the only reason (or basis) is Research or planning purposes. Patients may find out more at [nhs.uk/yournhsdatamatters](http://www.nhs.uk/yournhsdatamatters). The pharmacy will not process data if planning/research is the only reason for processing that data. The pharmacy therefore aligns with the opt-out system.

**Monitoring this policy**

This policy will be reviewed at least annually.

**Sanctions**

Breach of this policy could lead to disciplinary action. Depending on the circumstances this could range from remedial training to dismissal.

|  |
| --- |
| *This data security document assists the pharmacy’s aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies and more can be found at:** [*psnc.org.uk/ds*](http://psnc.org.uk/ds)*;*
* [*psnc.org.uk/dsptk*](http://psnc.org.uk/dsptk)*; and*
* [*psnc.org.uk/dstemplates*](https://psnc.org.uk/dstemplates)*.*

*Pharmacy contractors with queries about the original template or questions about DSPTK may contact* *it@psnc.org.uk**.* *This document is based on a template updated during: Feb 2021* |