

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Smartcard terms compliance template SOP** | | | | <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)*.* |  |

*This document sets out the communication, monitoring and enforcement processes that are in place to ensure that staff members comply with the NHS national application Smartcard terms and conditions of use (RA01 terms).*

**Communication**

When staff received their Electronic Prescription Service (EPS) Release 2 Smartcard, they will have been made aware of the RA01 terms and conditions and their responsibilities regarding Smartcard usage. Over time, the terms and conditions may change and Smartcard users will be asked to accept the changes through their computer software. If staff members need access to a current copy of the terms and conditions they can request this from the local NHS England team at any time.

All staff members that have EPS Release 2 Smartcards are asked to sign a staff signature list to confirm that they have read the terms and conditions and understand their responsibilities regarding Smartcard usage.

Annual reminders are issued to staff on the terms and conditions and staff responsibilities.

**Monitoring**

Monitoring to ensure that staff understand and are complying with the terms and conditions of smartcard usage is monitored through audit checks e.g. at least every year. The standard pharmacy IG audit checklist is used.

**Enforcement**

Staff members have been made aware that, where they have been issued with NHS Smartcards, they need to comply with the terms and conditions set down by the NHS for use of these cards. If staff members are found to not be complying, for example if this is identified through audit checks, the pharmacy’s standard disciplinary procedures will be followed as outlined in the Staff Confidentiality Code. Depending on the circumstances, sanctions range from remedial training to dismissal. Prosecution or an action for civil damages may also be taken under the data protection laws.

|  |
| --- |
| *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*](mailto:it@psnc.org.uk)*.*  *This document is based on a template updated during: Feb 2021* |