

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Data security and IG internal audit checklist** | | | | <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 may be used by the IG lead to help with data security audits. The topics may also assist with (a) training session(s) amongst the staff within the pharmacy.

***Note: Maintaining data security during ongoing pandemics****: It is recommended during ongoing pandemics that any audits being conducted by staff not usually working within the pharmacy building, are conducted remotely e.g. by phone call(s), email(s) and video meeting(s). Data security can be maintained remotely during or after pandemics.*

|  |  |
| --- | --- |
| **Testing of continuity issues: consider the scenarios below. In some cases a contingency paper process may be needed** | |
| Confirmed that staff and the IG/IT lead is aware what to do and who to contact if the phone or internet fails. |  |
| Confirmed that staff and the IG/IT lead is aware of the plan if the [Patient Medical Record (PMR) system](https://psnc.org.uk/supplierlist) fails. |  |
| Confirmed that staff know what would be done if there was a power outage? |  |
| Confirmed that staff know what would be done if the pharmacy were hacked? |  |
| Do all staff know how to contact key suppliers [e.g. those listed within the business continuity plan]? |  |
| Are policies and processes matching the continuity plan [note templates at: [/bcp](https://psnc.org.uk/bcp)] |  |
| The continuity plan is tested at least once per year [e.g. completion of this audit checklist section] |  |

|  |  |
| --- | --- |
| **Routine staff monitoring & compliance spot checks** | |
| Confirmed that staff members know where to find the Data security and IG policy and the purpose of the policy |  |

|  |  |
| --- | --- |
| **Data security training for staff** | |
| Confirmed every staff member has received their annual data security training including information on data quality (e.g. training by review of the [DSPTK Template-17-Data-Quality-Policy](https://psnc.org.uk/igtemplates)). Training materials are found at: [psnc.org.uk/dstraining](https://psnc.org.uk/dstraining). |  |
| Confirmed staff members understand their responsibilities (e.g. checked staff understand the confidentiality code of conduct) |  |

|  |  |
| --- | --- |
| **Leavers and IT logins/rights** | |
| Confirmed that the list of those persons with IT logins (available within some systems) includes those that may be working within the pharmacy. This is particularly relevant for any sensitive cloud systems. |  |
| Confirmed that those persons who have left employment during the last year have had their IT logins revoked – including their personal NHSmail accounts delinked from the pharmacy shared mailbox |  |

|  |  |
| --- | --- |
| **Staff understanding of confidentiality code of conduct** | |
| Confirmed that staff members know where to find the pharmacy’s confidentiality code of conduct and the purpose of the Code. |  |
| Confirmed that staff members know who the pharmacy Information Governance lead is and who to contact for support on data security issues. |  |
| Confirmed that staff know not to look at information about any patient including any information relating to their own family, friends and acquaintances unless they are directly involved in the patient’s care or with administration on behalf of the pharmacy. |  |
| Confirmed that staff members know that patient information should not normally be shared without patient consent. |  |
| Confirmed that staff working off-site or at home know not to remove patient identifiable information from the pharmacy. |  |

|  |  |
| --- | --- |
| **Compliance with Smartcard expectations** | |
| Confirmed that through questioning staff are not passing their Smartcards to other members of staff. |  |

|  |  |
| --- | --- |
| **Security measures** | |
| Confirmed that security alarm is being set each evening as per security arrangements |  |
| Confirmed that windows and doors are being locked each evening as per the security arrangements |  |
| Confirmed that staff know who to contact in the event of unauthorised access to information |  |

|  |  |
| --- | --- |
| **Review of compliance with mobile computing guidelines** | |
| Anti-virus has been recently updated or auto updates |  |
| Back-ups recently updated |  |
| The device contains no unauthorised software (or unauthorised software has related mitigating measures documented) |  |
| The device is being appropriately stored |  |
| The record of ownership of work mobile devices is up to date |  |

|  |  |
| --- | --- |
| **Incident management and reporting procedure** | |
| Confirmed that staff members know who to report suspicious incidents to |  |
| Confirmed staff know where the procedures can be located for managing different types of incident |  |

|  |  |
| --- | --- |
| **Compliance with access control SOP** | |
| Confirmed that only staff regularly working at the pharmacy regularly have active user profiles |  |
| Checked that no evidence of staff not following the procedures e.g. not using the username/password issued to them |  |

|  |  |
| --- | --- |
| **Access to computer-based information systems** | |
| Confirmed that individual staff members have access rights appropriate to their role |  |
| Where users no longer require access to the system, confirmed that their rights have been revoked |  |

|  |  |
| --- | --- |
| **Compliance with Safe Haven Procedures** | |
| Is personal information being moved from the front counter to the secure dispensary area as soon as practical? |  |
| Are patient records such as service consent forms being stored securely when not in use? |  |
| Is the security of password(s) to access the key clinical system(s) being maintained (i.e. passwords not written down and left beside the computer) |  |
| Is patient returned waste which includes personal information (e.g. waste medicine boxes with labels) being put into the controlled waste (DOOP) bin as soon as practically possible or alternatively labels shredded as required by the pharmacy procedures? |  |
| Do staff members ensure that sensitive conversations with patients are not overheard? |  |

|  |  |
| --- | --- |
| **Review of compliance with data transfer procedures** | |
| Are envelopes containing personal information being marked ‘Private & Confidential’? |  |
| Confirmed that personal information is not being sent via email other than from NHSmail addresses to NHSmail addresses? |  |
| Are prescriptions being sent to NHSBSA (Pricing Authority) using a ‘track and trace’ service? |  |
| When providing information over the telephone is the callers identify always confirmed? |  |
| Confirmed that staff members are not copying any personal information to unencrypted memory sticks? |  |

|  |
| --- |
| **Notes:** |

|  |
| --- |
| *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* |