

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Information security incident management procedures** | | | | <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)*.* |  |

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the information through the system being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to authorised access to data.

**Procedures for dealing with various types of incident**

All staff should report any suspicious incidents to [enter details e.g. the IG lead in the premises and/or within the organisation].

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be co-ordinated by [the IG lead in the premises and/or within the organisation depending on the seriousness of the incident].

The following procedures should be followed for particular breaches:

1. **Theft of equipment holding confidential information and unauthorised access to an area with unsecured confidential information:**

* Check the asset register to find out which equipment is missing.
* Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base).
* If the cause is external inform the Police and ask them to investigate.
* If the cause is internal, establish the reason for the theft/ unauthorised access.
* Consider the sensitivity of the data and the risk that it will be misused, to support assessing whether further action is appropriate (e.g. warning patients, informing the Police, local NHS England and NHS Improvement team).
* Consider whether there is a future threat to system security and the need to take protective action e.g. change passwords.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

1. **Access to patient records by an authorised user who has no work requirement to access the record:**

* Interview the person reporting the incident to establish the cause for concern.
* Establish the facts by;
  + Asking the system supplier to conduct an audit on activities by the user concerned.
  + Interviewing the user concerned.
* Establish the reason for unauthorised access.
* Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
* Take appropriate disciplinary action and action with the patient(s) where appropriate.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

1. **Inadequate disposal of confidential material (paper, PC hard drive and disks):**

This type of incident is likely to be reported by a member of the public, a patient affected, or a member of staff;

* Investigate how the data came to become inappropriately disposed.
* Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
* Take appropriate action to prevent further occurrences. (e.g. disciplinary, advice/training, contractual)
* Take appropriate action with the patient(s) as appropriate.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

1. **Procedure for dealing with complaints about patient confidentiality by a member of the public, patient or member of staff:**

* Interview the complainant to establish the reason for the complaint (Note, any complaint by a patient in relation to his NHS services must be investigated and handled in accordance with the Terms of Service).
* Investigate according to the information given by the complainant and take appropriate action.
* Take appropriate action with the patient(s) as appropriate.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

1. **Loss of data in transit e.g. when posting NMS forms to the GP surgery or sending prescriptions to NHSBSA:**

* Investigate, as far as possible what has gone missing and where.
* Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
* Take appropriate action to prevent further occurrences. (e.g. process (was the envelope correctly addressed, is there further safeguards that could be introduced).
* Take appropriate action with the patient(s) as appropriate.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

**Procedures for recording incidents**

A record of all incidents, including near-misses, should be made by completing a copy of the information security incident report form.

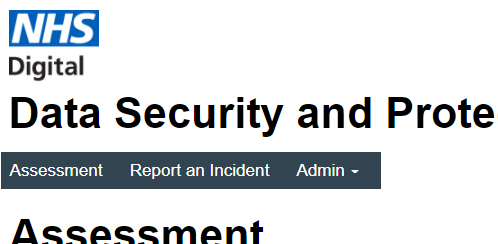
Incidents should be classified in the log according to severity of risk to patients and the pharmacy using the following incident classification system described below. For near-misses, consider the likely impact if the breach had occurred.

**Incident Classification:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insignificant:**  Minimal discernible effect on patients or the pharmacy. | **Minor:**  Minor breach, for example data lost but files encrypted, less than 5 patients affected.  **Inconvenient to the pharmacy but manageable.** | **Moderate:**  Moderate breach, for example unencrypted clinical records lost, up to 20 patients affected.  **Potential for damage to the pharmacy’s reputation.** | **Major:**  Serious breach, for example unencrypted clinical records lost, up to 1,000 patients affected or particular sensitivity e.g. sexual health information disclosed.  **Potential for damage to the pharmacy’s reputation and/or local media coverage.** | **Critical:**  Serious breach in terms of volume of records, for example over 1,000 patients affected or particular sensitivity of records.  **Damage to the reputation of the NHS and the pharmacy profession. Potential for national media coverage.** |

**Procedures steps**

Incidents should be reported to person listed above.

This person will determine whether there is also a need to report the incident to others depending on the type and likely consequences of the incident, e.g.:

* Using the ‘*Report an Incident*’ option from within the Data Security and Protection Toolkit account (see image to right). NHS Digital may also forward information onwards where that is needed.
* Inform the Police.
* Inform the local NHS England and NHS Improvement team.
* Inform the pharmacy’s insurer.
* Etc.

Although there may not be legal requirement to do this, where there is high risk of harm to patients, it is considered best practice to also inform the Information Commissioner.

|  |
| --- |
| *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* |