LINDSEY LODGE HOSPICE & HEALTHCARE

Data Security Breach Management Policy

LINDSEY LODGE HOSPICE & HEALTHCARE

DATA SECURITY BREACH MANAGEMENT POLICY

Lindsey Lodge handles a significant amount of data which must be handled securely by law. A breach in the secure handling of information can carry a monetary penalty of up to £500,000, which can be served and enforced by the Information Commissioner's Office (ICO).

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attach
- 'blagging' offences where information is obtained by deceiving the organisation which holds it
- Access by an unauthorised third party

Management of a breach

There are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

ACTIONS

1. **Containment and recovery**
   If any member of staff discovers a breach of information, they must immediately notify a member of the Information Governance (IG) team (Kay Fowler – Data Protection Officer, Dr Lucy Adcock – Caldicott Guardian, Karen Griffiths – Senior Information Risk Officer).

   In the event of the discovery of the breach occurring out of normal working hours depending on the severity of the breach, a senior manager must be informed immediately, otherwise wait until normal working hours. However, the containment and recovery of information must not wait until office hours and attempts to do this must be made straight away.

   It is often difficult to determine risks associated with a breach to understand severity and if there is a need to discuss this in and out of hours any member of the IG team can be contacted at any time

2. Assessing the Risk

This involves an assessment of the potential adverse consequences for individuals. Points to consider:

- What type of data is involved?
- How sensitive is it; e.g. personal information (health records, bank details?
- If data is lost or stolen, are there any protections (e.g. encryption)?
- What has happened to the data - lost, stolen, damaged?
- What could the data tell a third party about the individual(s)?
- How many individuals are affected?
- Who are the affected individuals – staff, patients, clients, suppliers?
- What harm can come to those individuals?
- Are there wider considerations – e.g. to public health, loss of public confidence?
- Consider contacting the bank if details lost as they may have further advice.

3. Notification of the breach(es)

Inform the people and organisations which have experienced the data security breach. They may need to take certain steps to protect themselves further. This will also allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

The appropriate regulatory body needs to be informed (CQC for patient related data security breaches as well as the ICO for personal data breaches).

Any data security breach needs to be logged on Lindsey Lodge incidents database held on the L drive, Incidents, by the person identifying the breach. A member of the IG team will then investigate the breach fully and update with action taken/lessons learnt.

Following amendments to the Data Protection Act when a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms needs to be accessed. This will be completed by the Data Protection Officer or Caldicott Guardian who will use the Data Security & Protection Scoring tool held on the L drive to assess the risk of recurrence and the consequence grading.

If it's likely that there will be a risk then the data protection officer must notify the ICO within 72 hours of being identified; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision.
There is further guidance on the ICO website on how to report a breach
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

4. Evaluation and response

It is important with any breach of information to evaluate what happened, review policies and procedures to identify where improvements need to be made.

Whilst the organisation has a management structure to facilitate secure and appropriate handling of data, individual staff are also responsible for reporting of any potential risk to data handling.

The incident will be investigated by relevant persons identified by the IG team and lesson learned and actions will be shared and cascaded to staff at team meetings and via Team Talk.

5. Consultation

IT & IG committee

6. Dissemination

Via Lindsey Lodge `L` drive policies/guidelines of this form.

7.0 Equality Act

In accordance with the Equality Act (2010), Lindsey Lodge will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage.
Lindsey Lodge will endeavour to develop an environment within which individuals feel able to disclose any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

Lindsey Lodge will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

Policy Author: Dr Lucy Adcock October 2016; Review 2 yearly Ratified QA 26th January 2017				
ISSUE DATE October 2016 , review 2 yearly				
TO BE REVIEWED	REVIEW COMPLETED	BY	APPROVED BY	CIRCULATION
October 2018	February 2019	Kay Fowler	IT & IG committee	All staff have access to L: Policies & guidelines
February 2021	April 2021	Kay Fowler	IT & IG committee	All staff have access to L: Policies & guidelines
April 2023				