SoHPS

Society of Health Play Specialists

DATA PROTECTION BREACH

REPORTING PROCEDURE

INTRODUCTION

Background

The NHS Information Governance Tool Kit which is being adopted by Society of Health Play Specialists (SoHPS) will be used to identify and assess any breaches in data protection related to the Data PROTECTION Act 1998 and General Data Protection Regulations 2018 and subsequent amendments. This Information Governance Toolkit is a performance tool produced by the Department of Health. Its' purpose is to enable organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Purpose

The purpose of an incident response is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the SoHPS board, as appropriate, who will work to prevent future incidents.

2. INCIDENT MANAGEMENT

Definition

A Data Protection breach is the result of an event or series of events where Personally Identifiable Information is not stored, destroyed or shared with person(s) correctly and can be viewed by persons not entitled to view the data

Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

REPORTING MECHANISMS FOR SoHPS

SoHPS Board will: -

- Put measures in place to ensure that awareness of data protection will enable breaches to be reported
- Issue guidance on how to report data breaches
- Ensure that its contemporaneous logs of incidents are kept
- Recommendations and lessons learnt from any data breach to be shared to prevent reoccurrence

Process for Data breaches

Diagram below shows the flow of actions involved in a data breach review

Reporting

2.4.1 The objective of any breach investigation is to identify what actions the organisation needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the Information

Commissioner's Office.

Lessons Learned

Key to preventing further incidents is ensuring the organisation learns from an incident.

OUTLINE PROCEDURE FOR INCIDENT HANDLING

On identification of a breach of the personal data, a review will be undertaken. The individual must be notifying of the breach as soon as identified and of the outcome of the review any actions put into place to prevent a future occurrence or mitigation of the risk.

Any data breaches need to be logged and reported immediately to the Chair and the Data protection officer for action to be taken within 72 hours of the report.

Data Protection Breach Reporting Form

The aim of this document is to ensure that in the event of a data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk.

1. Summary of Incident	
Date and Time of Incident	
Number of people whose data is affected	
Nature of breach – actual data lost or corrupted	

Description of how breach occurred	
Date and time breach reported	
What immediate remedial action was taken - Has the data been retrieved or deleted? If yes - date and time:	

Feedback, Lessons Learnt and recommendations	
Date / Signature of person(s) completing review and follow -up.	