Standard Operating Procedure (SOP)

INFORMATION GOVERNANCE INCIDENT MANAGEMENT

SETTING	Trustwide
FOR STAFF	All staff must read "Identifying and Reporting an Information Governance Incident", and incident investigators and divisional governance leads must read the whole SOP
ISSUE	This SOP describes the process to identify, record, investigate and remedy incidents relating Information Governance

Standard Operating Procedure (SOP)

This SOP is to be read in conjunction with the Trust Incident Recording and Management SOP (link when published) and relates solely to incidents affecting the confidentiality, integrity or availability of information in any format.

Regulatory Background and Associated Guidance

Article 32 of the UK GDPR places the responsibility on all organisations processing personal data to implement appropriate organisational and technical measures to ensure an appropriate level of security to the personal data they process.

Article 33 of the UK GDPR places the responsibility on all organisations processing personal data to report incidents that are likely to result in detriment to the individuals involved to the Information Commissioner's Office within 72 hours of becoming aware of them.

Article 34 of the UK GDPR places the responsibility on all organisations processing personal data that where an incident is likely to result a high risk of detriment to the individuals involved, the organisation shall inform the individual of the incident.

Part 3, Regulation 11 of the Network and Information Systems (NIS) Regulations places the responsibility on essential services (including healthcare) to have appropriate levels of security and to report any incident affection networks or information systems which has a significant impact on the continuity of service provision.

NHS Digital (now merged with NHS England) produced a Guide to the Notification of Data Protection and Security Incidents in conjunction with the Information Commissioner's Office to assist NHS organisations with identifying, grading and reporting high risk incidents. This guidance is the basis of the Trust's Information Governance Incident Management SOP.

Definitions

Personal Data – Any information relating to an identified or identifiable living individual

Data Breach – Any incident where the confidentiality, integrity or availability of personal data is affected

Confidentiality Breach – Unauthorised or accidental disclosure of, or access to personal information

Integrity Breach – Unauthorised or accidental alteration of personal information

Availability Breach – Unauthorised or accidental loss of access to or destruction of personal information

Supervisory Authority – The Information Commissioner's Office (ICO) is the national data protection authority in the UK.

Identifying and Reporting an Information Governance Incident

An Information Governance incident, or data breach, is any incident that affects the confidentiality, integrity or availability of information, examples of which are:

Confidentiality	Integrity	Availability
Data sent to incorrect recipient	Misfiling of paper records	Loss or theft of paperwork
Unauthorised access to records	Electronic records uploaded to the wrong person	Loss or theft of IT device
Failure to redact data	Unauthorised or accidental alteration of data	Insecure disposal of data
Accessing records outside the scope of your job role		Network outage
Upload of information to non-Trust approved apps, systems or websites		Wrongful encryption of electronic data (e.g. ransomware)
		Denial of service attack

When an Information Governance Incident has been identified you must follow the steps outlined in the Trust Incident Recording and Management SOP (link when published). When an incident contains a data breach, the incident recorded must include wherever possible:

- What data has been breached, and what does this contain
- The amount of data that has been breached
- How the data was breached
- Any reported or expected effect to the individual or to the provision of services

When recording incidents, only one category and subcategory can be chosen, you must choose the most appropriate options to describe the incident. However, an incident may also include a breach to the confidentiality, integrity or availability of information. In this case, you can also choose to add the Information Governance Team to "Should a Specialist Team be made aware of this incident?" when recording the incident on Datix.

Managing Information Governance Incidents

Where an incident affects the confidentiality, integrity or availability of information there must be an investigation of that data breach by the incident handler even if other aspects of the incidents

do not reach the investigation thresholds identified in the Trust Incident Recording and Management SOP (link when published).

The steps to manage any data breach by the incident handler are as follows:

1. Assess the recorded incident on Datix and take mitigating actions to contain the data breach (e.g. ask for an incorrect recipient to destroy the information, contact IT to report ransomware or phishing emails)
2. Ensure Information Governance are aware of the incident as soon as possible by adding them as a "Specialist Team" to the incident record on Datix or by marking "Is there an Information Governance element to this incident" in the "Information Governance tab as "Yes"
3. Review the incident and identify the cause (e.g. is there a training need, an issue with systems or processes, pressures causing staff to rush tasks)
4. Implement actions to prevent recurrence of the data breach and ensure any relevant learning is shared with wider teams
5. Ensure all of this information is recorded on Datix

Where Information Governance are made aware of data breaches they will:

1. Conduct an initial review of the recorded data breach on Datix and request that any missing information is added to the incident record
2. Make an initial assessment of risk of detriment to the individuals involved based on:
    - The circumstances of the data breach
    - The type of data breached
    - The amount of data breached
    - The effect it has on the individuals involved
    - The effect it has on the provision of services
3. Conduct an initial scoring of the incident in line with the NHS Digital Guide to the Notification of Data Protection and Security Incidents as soon as possible, and complete the scoring fields in the "Information Governance" tab
4. If the incident does or is likely to meet the threshold for reporting to the Information Commissioner's Office, progress to "Managing High Risk Information Governance Incidents".
   OR
4. If the incident does not or is not likely to meet the threshold for reporting to the Information Commissioner's Office, offer advice to the incident handler who manages and closes in line with the above steps and the Trust Incident Recording and Management SOP (link when published)

Managing High Risk Information Governance Incidents

Any data breach that is likely to cause detriment to the individuals involved is classified as a High Risk Information Governance Incident. Examples of detriment are:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft, Fraud or Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy

- Other significant economic or social disadvantage to individuals

Where the Information Governance Team have made an initial assessment that the incident does or is likely to meet the threshold for reporting to the Information Commissioner's Office the following steps will be taken by the Information Governance Team:

1. Notify the Divisional Governance Team or Departmental Managers of a potential High Risk Information Governance Incident and advise on any further investigation or information required, involving other subject matter experts where required.
2. Ensure that any measures that could be taken to contain the data breach have been taken or are planned following further investigation.
3. Start the draft Incident Notification on the Data Security and Protection Toolkit (DSPT) Website, completing all required fields as listed in Appendix 4 of the NHS Digital Guide to the Notification of Data Protection and Security Incidents and save, but do not submit.
4. Circulate the draft Incident Notification (a pdf version can be downloaded from the website following saving) to the relevant stakeholders to confirm accuracy, updating the draft version on the DSPT website as required.
5. Circulate a final version of the Incident Notification to the Data Protection Officer, Caldicott Guardian and Senior Information Risk Owner for approval
6. Once approved, submit the Incident Notification on the DSPT website and record any received reference numbers in the "Information Governance" tab on Datix. This is required before the 72 hour notification deadline. If this step is completed after 72 hours since the Trust was aware of the incident, then an explanation of the delay will also be required.

Once the Incident Notification is submitted on the DSPT Website, a copy is automatically sent to NHS England and the Information Commissioner's Office. The Information Commissioner's Office will review the incident notification and will usually respond with a set of additional questions for the Trust to answer to assist with their investigation.

7. On receipt of the Information Commissioner's Office's additional questions, coordinate the response with the Incident Handler, subject matter experts and additional stakeholders within the timeline set out by the caseworker. This step may repeat until the caseworker can conclude the investigation.
8. On receipt of the Information Commissioner's Office's decision, circulate the decision and ensure any additionally identified actions are planned or complete.
9. Populate the Datix entry for the incident with all additional information, ensuring it is accurate and complete.

Following these final steps, the incident handler can close the incident on Datix if all other aspects are complete.

Internal Governance and Escalation

- Divisional Reports to Information Risk Management Group will highlight High Risk Information Governance Incidents, and request formal closure of internal action plans relating to these incidents in line with the Terms of Reference
- Information Risk Management Group will provide summaries of these incidents in it's onwards reporting as defined in its Terms of Reference
- A summary of all reported High Risk Information Governance Incidents will be included in the Trust's Annual Report

Appendix 1 – Evidence of Learning from Incidents

The following table sets out any incidents/cases which informed either the creation of this document or from which changes to the existing version have been made.

Incidents	Summary of Learning
None	

Table A

REFERENCES	UK GDPR Ch 4, Section 2 Guide to the Notification of Data Protection and Security Incidents, NHS Digital Guide to UK GDPR, Information Commissioner's Office
RELATED DOCUMENTS AND PAGES	Information Governance Policy Data Protection Policy Confidentiality Policy Trust Incident Recording and Management SOP (link when published) Information Security Policy
AUTHORISING BODY	Information Risk Management Group
SAFETY	None
QUERIES AND CONTACT	Information Governance, InformationGovernance@UHBW.nhs.uk
AUDIT REQUIREMNTS	Notification of High Risk Information Governance Incidents to Information Risk Management Group – Quarterly Annual Summary of reported High Risk Information Governance Incidents in the Annual Report Annual Summary of Incident Trends and compliance with the 72 hour notification deadline to Information Risk Management Group

Plan Elements	Plan Details
The Dissemination Lead is:	Information Governance
Is this document: A – replacing the same titled, expired SOP, B – replacing an alternative SOP, C – a new SOP:	B
If answer above is B: Alternative documentation this SOP will replace (if applicable):	Information Governance Serious Incident SOP
This document is to be disseminated to:	Divisional Governance Teams and All Staff
Method of dissemination:	Newsbeat and email to Divisional Governance Teams
Is Training required:	Covered in Annual IG Essential Training

Document Change Control

Date of Version	Version Number	Lead for Revisions	Type of Revision	Description of Revision
Mar 22	3.00	Information Governance Manager	Major	Last full review of the SOP, updated to reflect new structures and job roles
Jun 23	4.00	Information Governance Manager	Major	Updated to reflect changes to incident management following implementation of Patient Safety Incident Response framework