

Procedure

Information Governance Incidents and Investigation

1 Scope

This policy applies to all Trust employees, including:

- staff who hold honorary contracts;
- contractors working on behalf of the Trust;
- the Board of Governors;
- Non Executive Directors.

2 Purpose

- standardise the procedures for information governance investigations;
- ensure compliance with relevant legislation;
- to ensure that any lessons learnt from incidents are implemented.

3 Introduction

This procedure describes the stages to be followed in the event of an information governance investigation into either computer activities of an individual, a suspected or actual information security breach, a breach of confidentiality or a breach of the Data Protection Act 1998. For examples of incidents please refer below, this list is not exhaustive.

- virus outbreaks;
- theft or damage to computer equipment;
- access or attempted unauthorised access to computer systems;
- viewing or downloading inappropriate material;
- attempted or actual fraud.
- unauthorised disclosure of information;
- unauthorised obtaining of data;
- unauthorised destruction or deletion of data;
- accessing patient information to which not entitled to do so;
- faxing information to wrong number;
- loss or theft of personal identifiable information;
- mentioning someone attended the hospital;
- discussion about patient(s) within or outside of the hospital;
- reading health record when no requirement to do so.

It is important to note that if at any time during the process described below, either fraud, paedophilic images or criminal activity is suspected or confirmed then all investigations must cease and either the Trust Counter Fraud Officer or Trust Security Advisor must be informed.

It is important to keep as much information as possible of the incident and investigation confidential. No information should be discussed with anyone who is not directly involved with the incident.

4 Definitions

Data controller: This is the person or organisation who either alone or jointly or in common with other persons determines the purpose for which and the manner in which any personal data is processed.

Information Governance Serious Untoward Incident (SUI): any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious.

Information Commissioner's Office: an independent body who oversees compliance with the Data Protection Act and undertakes investigations into the breaches of the Act.

Personal identifiable data (PID): PID that relates to a living individual who can be identified from that data or from that data and other information that is in the possession of or is likely to come in the possession of the data controller (The Trust). These items include surname, initials, date of birth, address and postcodes, sex, national insurance number, hospital number, forenames, occupation, NHS number, ethnic group. This is not an exhaustive list, personal data can be information that does not include any of these personal details but the individual could be identified from this information and other information in possession of the data controller by association e.g. medical photograph of a patient with a rare condition.

5 Computer Investigations

The IT Department is responsible for investigating computer incidents and the IT Information Governance Lead should be informed about the incident.

If the computer activity incident involves PID, the investigation should be undertaken by the IT Information Governance Lead and Information Governance Lead, please refer to section 6.

If an incident relates to a specific PC, ensure that no one can use the PC until it has been examined by either moving the PC or placing a note on the PC. If the incident relates to an individual they should not be informed at this stage.

The procedure to be followed is

1. An incident form must be completed;
2. If the incident could result in disciplinary action against a member of staff then the HR patch manager must be consulted;

Further investigation required:

4. Before any equipment can be removed or log files examined a brief description of the incident and scope of what is to be checked must be approved by the Department Manager and or HR Patch Manager;
5. during the investigation all activity must be recorded, including files examined or web sites checked;
6. examination of PC disks involving any changes to data should be carried out on a copy of that data, keeping the original disk secure;
7. produce a report of the findings of the investigation, this may form part of the HR investigation file;
8. identify any actions to avoid the incident from occurring again in the future, ensure these actions are undertaken.

6 Breaches of Confidentiality and Data Protection

The Information Governance Lead will be copied into all incidents relating to confidentiality and Data Protection. All incidents will be reviewed by the Information Governance Lead.

For actual or potential data losses please refer to the Data Loss section below.

- incident form must be completed;
- establish the facts of the incident, what happened, where and how and who was involved;
- check if any staff involved have signed compliance with the Chief Executive's letter issued February 2008 or the information governance code of conduct for new starters and the date they last completed their mandatory information governance training;
- establish whether further investigation is appropriate, discuss with Departmental Manager;
- identify any lessons learned from the incident, take appropriate action to implement;
- record the incident on the 'Incident Log'

Data or Potential Losses of personal identifiable data:

- incident form must be completed;
- inform the Information Governance Lead or Head of Patient Services of the data loss;
- establish the facts of the incident, what happened, where and how and who was involved;
- check if any staff involved have signed compliance with the CE Letter issued February 2008 or the Information Governance Code of Conduct for new starters and the date they last completed their mandatory information governance training ;
- record the incident on the Incident Log;
- keep a record of all activity relating to the investigation, the information governance team will hold all records relating to the SUI;
- in consultation with Risk Management consider whether the incident should be classed as a SUI level 1 to 5, please refer to Appendix 1;

Score 0 – not classed as a SUI

- record decision on incident log;
- establish whether further investigation is appropriate, discuss with Departmental Manager;
- identify any lessons learned from the incident, take appropriate action to implement.

Score 1-2: reported as an SUI

For additional guidance please refer to flow chart at Appendix 2

- record decision on incident log;
- inform the Director of Information Systems and Analysis;
- identify and manage the risks of the incident and consequence risks of the incident, where appropriate the Information Governance Lead will undertake the risk assessments;
- complete the SUI form and the additional Data Loss form for the PCT, Risk Management will send the SUI forms to the PCT;
- the investigation will either be undertaken by the Information Governance Lead/Data Protection Officer or the Department Manager or jointly, an action plan will be produced including a communication plan, the implementation of the action plan will be monitored by the Director of Information Systems and Analysis and the Information Governance Steering Group where appropriate;
- HR Patch Manager to be consulted by Departmental Manager if disciplinary action is being considered;
- establish the root causes for the incident, identify any lessons learnt, include in the SUI action plan to ensure lessons learnt are implemented;
- produce root cause analysis report, circulated to Risk Management and the Information Governance Steering Group for monitoring.

Score 3-5: reported as an SUI

For additional guidance please refer to flow chart at Appendix 2

- record decision on incident log;
- inform the Director of Information Systems and Analysis;
- convene the Data Loss meeting, Appendix 2 identifies the members who must attend this meeting, this meeting will agree the following:
 - identify who will undertake the investigation and any actions to establish the full facts of the incident;
 - in consultation with HR agree the appropriate course of action for any potential disciplinary investigations;
 - decide whether the individuals whose data has been lost should be informed of the data loss and the approach this should take;
 - agree the communication plan;
 - agree the action plan for the investigation;
 - identify and manage the risks of the incident and consequence risks of the incident, where appropriate the Information Governance Lead will undertake the risk assessments
- complete the SUI form and the additional Data Loss form for the PCT, Risk Management will send the SUI forms to the PCT;
- the Data Protection Officer will draft and send the letter to the ICO to inform them of the incident;

- the action plan will be monitored by the Director of Information Systems and Analysis and the Information Governance Steering Group;
- establish the root causes for the incident, identify any lessons learnt, include in the SUI action plan to ensure lessons learnt are implemented;
- produce root cause analysis report, circulated to Risk Management and the Information Governance Steering Group for monitoring.

7 Disciplinary Procedures

Staff who breach the,

- Information governance policies and procedures identified below;
- the Data Protection Act;
- the Computer Misuse Act
- or breach patient Confidentiality

will face disciplinary actions in line with the Trusts Disciplinary policy and procedure which could lead to loss of employment

The Trust and individual employees can be prosecuted for offences under the Data Protection Act 1998 for:

- Processing personal data without notifying the Information Commissioner.
- Processing personal data for any purpose other than that covered by the Trust's notification.
- Unauthorised disclosure of personal data e.g. disclosure to a person/organisation not entitled to receive it.
- Failure to comply with an information/enforcement notice issued by the information commissioner.
- Modifying personal data as a result of a subject access request.
- Accidental loss or destruction or damage to personal data.

If the patient has suffered damage due to contravention of the Act they could be entitled to compensation. Individuals are entitled to seek compensation via the courts due to loss of data, unauthorised destruction of data or unauthorised disclosure of data.

The Trust and individual employees can be prosecuted for offences under the Computer Misuse Act 1990 for:

- unauthorised access to computer material (programs or data);
- unauthorised access to computer systems with intent to commit or facilitate the commission of a serious crime;
- unauthorised modification of computer material

8 Publishing results

SUI incidents will be reported in the Trust's annual report as required by the DH, please refer to Appendix 3 for the format this information must be provided in.

The Statement of Internal Control will include a description of how information risks are being managed by the Trust.

9 Monitoring compliance with and the effectiveness of this document

Key standard:

- all incidents are dealt with in accordance with this procedure

The standards will be monitored by the information governance team by:

- incidents will be reported in the information governance quarterly report that is received by the Information Governance Steering Group and the Information Systems Program Board;
- a log of all incidents will be maintained;
- all SUI action plans will be monitored via the Information Governance Steering Group to ensure any lessons learned are implemented.

Any issues raised by incidents will be communicated to staff through the information governance e-bulletin and included in the information governance training sessions as appropriate

10References

Data Protection Act

Computer Misuse Act

DH Checklist for reporting, managing and investigating information governance serious untoward incidents

East of England SHA SUI Policy

ICO – guidance on data security breaches management

ICO – notification of data security breaches to the ICO

11Associated documents

Data Protection Policy

Information Security Policy

Confidentiality of Personal Health Policy

Incident and Investigation Policy and Procedure

Disciplinary Policy and Procedure

Information Governance Policy

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is your responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Document management

Document draft tracking; table will be removed before publication					
Issue	Author(s)	Owner	Date	Circulation	Comments

Information Governance

Directorate of Information Systems and Analysis

Draft 1 (V1)	Information Governance Lead & IT Governance Lead	Information Governance	Jan 10	IGSG	Approved 9.2.10
Draft 2					
Draft 3					
Draft 4					

This table will be completed by the Trust Documents Team:

Approval:			
Owning department:			
Author(s):			
File name:	TEMPLATE Trust documents GENERIC Version1.3 November 2009.doc		
Supersedes:			
Version number:		Review date:	
Local reference:		Media ID:	

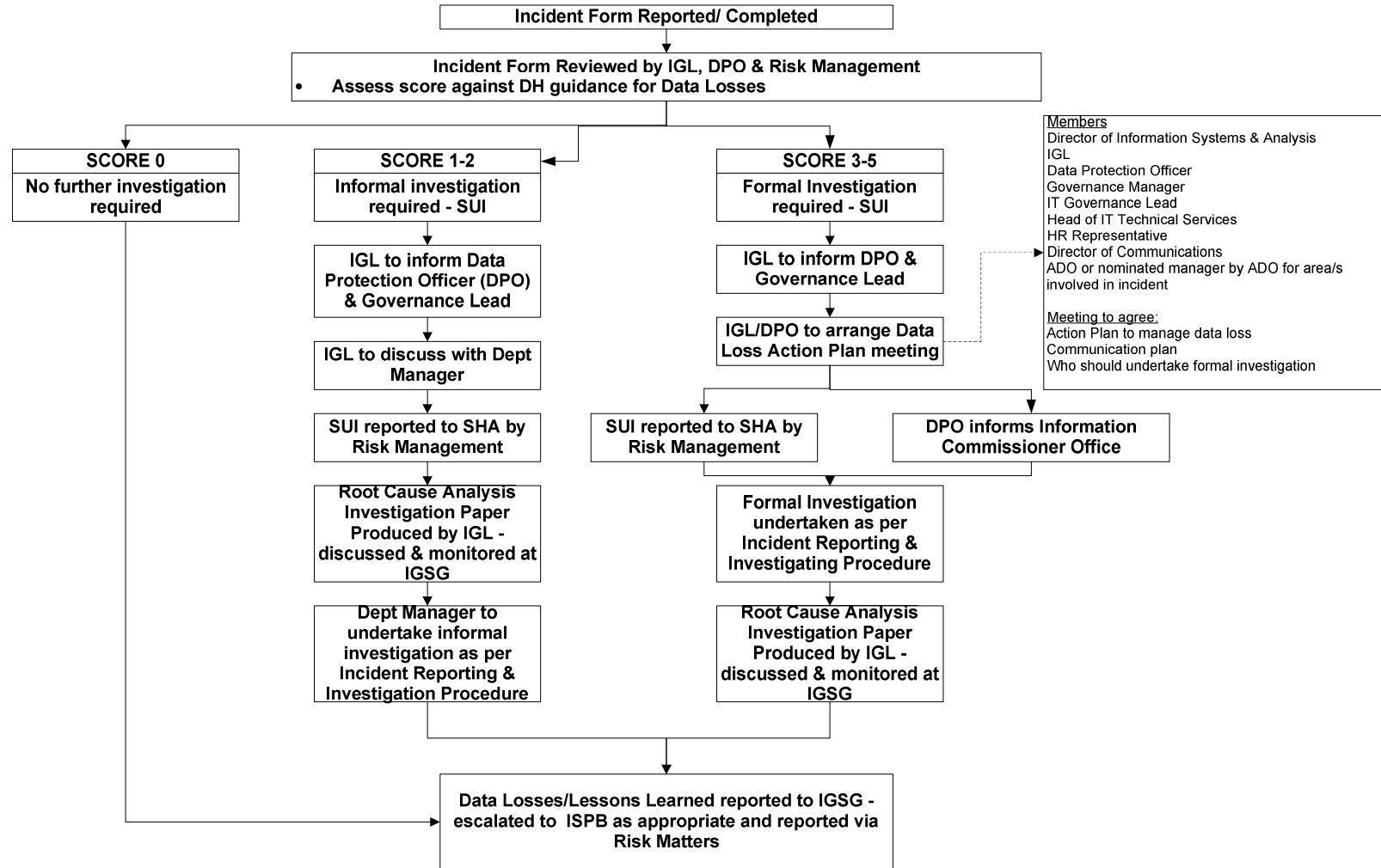
Template: Media ID: 328 Reviewed: 20 March 2010

Appendix 1: Serious Untoward Incident Categories

0	1	2	3	4	5
No significant reflection on any individual or body. Media interest very unlikely	Damage to an individual's reputation. Possible media interest e.g. celebrity involved.	Damage to a team's reputation. Some local media interest that may not go public	Damage to a services reputation. Low key local media coverage.	Damages to an organisations reputation. Low key local media coverage.	Damage to NHS reputation. National media coverage.
Minor breach of confidentiality. Only single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach & risk assessed as high e.g. unencrypted clinical records lost. Up to 20 people affected.	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details or up to 1000 people affected.	Serious breach with potential for ID theft or over 1000 people affected.

Appendix 2: Data Loss investigation flow chart

Data Protection Investigation Procedure



Appendix 3: Annual report SUI reports

Summary of Serious Untoward Incidents

Date of Incident	Nature of Incident	Nature of data involved	Number of people potentially affected	Notification Steps
Further action on Information risk				

Summary of other personal data related incidents

Category	Nature of Incident	Total
1	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	
2	Loss of inadequately protected electronic equipment, devices, paper documents from outside secured NHS premises	
3	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	
4	Unauthorised disclosure	
5	Other	