Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents

Gateway Ref: 13177

Information Governance Policy

Department of Health

Jan 2010

DH INFORMATION READER BOX

Policy	Estates
HR / Workforce	Commissioning
Management	IM & T
Planning /	Finance
Clinical	Social Care / Partnership Working

Document Purpose	Best Practice Guidance
Gateway Reference	13177
Title	Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents
Author	DH/Informatics Directorate/Information Governance Policy
Publication Date	
Target Audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs
Circulation List	
Description	Guidance for all NHS staff involved in managing an Information Governance Serious Untoward Incident. It should be used in conjunction with previously issued national guidance and local guidance issued by SHAs
Cross Ref	Matthew Swindells letter dated 20 Feb 2008
Superseded Docs	N/A
Action Required	N/A
Timing	**n/a**
Contact Details	Marie Greenfield Informatics Directorate, Room 1N24 Quarry House Leeds LS2 7UE 1133974408
For Recipient's Use	

1. Introduction

1.1 Matthew Swindells' letter of the 20th February 2008 (Gateway 9571) included guidance on the process for reporting Information Governance (IG) Serious Untoward Incidents and assessing their severity. This is included at Annex A.

1.2 The definition of an IG SUI given at paragraph 2 of Appendix A is:

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.

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

1.3 Experience of reporting and managing IG SUIs has indicated the need for additional guidance, support and clarification of the criteria to be used when evaluating IG SUIs. This guidance has been approved by all SHA IG leads and the DH Digital Information Policy Team. Particular thanks are owed to Clive Thomas, South Central SHA, as the principal author of this document.

2. Purpose of this Checklist

2.1 This checklist should be used in conjunction with the previously provided national guidance on the management of Serious Untoward Incidents and any local guidance on SUIs provided by your SHA. The intention is to ensure that:

- the management of IG SUIs conforms to the processes and procedures set out for managing all Serious Untoward Incidents
- there is a consistent approach to evaluating IG SUIs;
- early reports of IG SUIs are sufficient to decide appropriate escalation, notification and communication to interested parties;
- appropriate action is taken to prevent damage to patients, staff and the reputation of the NHS;
- all aspects of a SUI are fully explored and 'lessons learned' are identified and communicated; and
- appropriate corrective action is taken to prevent recurrence.

2.2 The checklist should be used by all staff involved in managing an IG SUI.

2.3 It is important to note that much of this checklist will be applicable to 'near misses. Staff should be encouraged to report IG SUI "near misses" and the opportunity taken to identify and disseminate the 'lessons learnt'.

2.4 All staff should know to whom they should report and escalate suspected or actual IG SUIs.

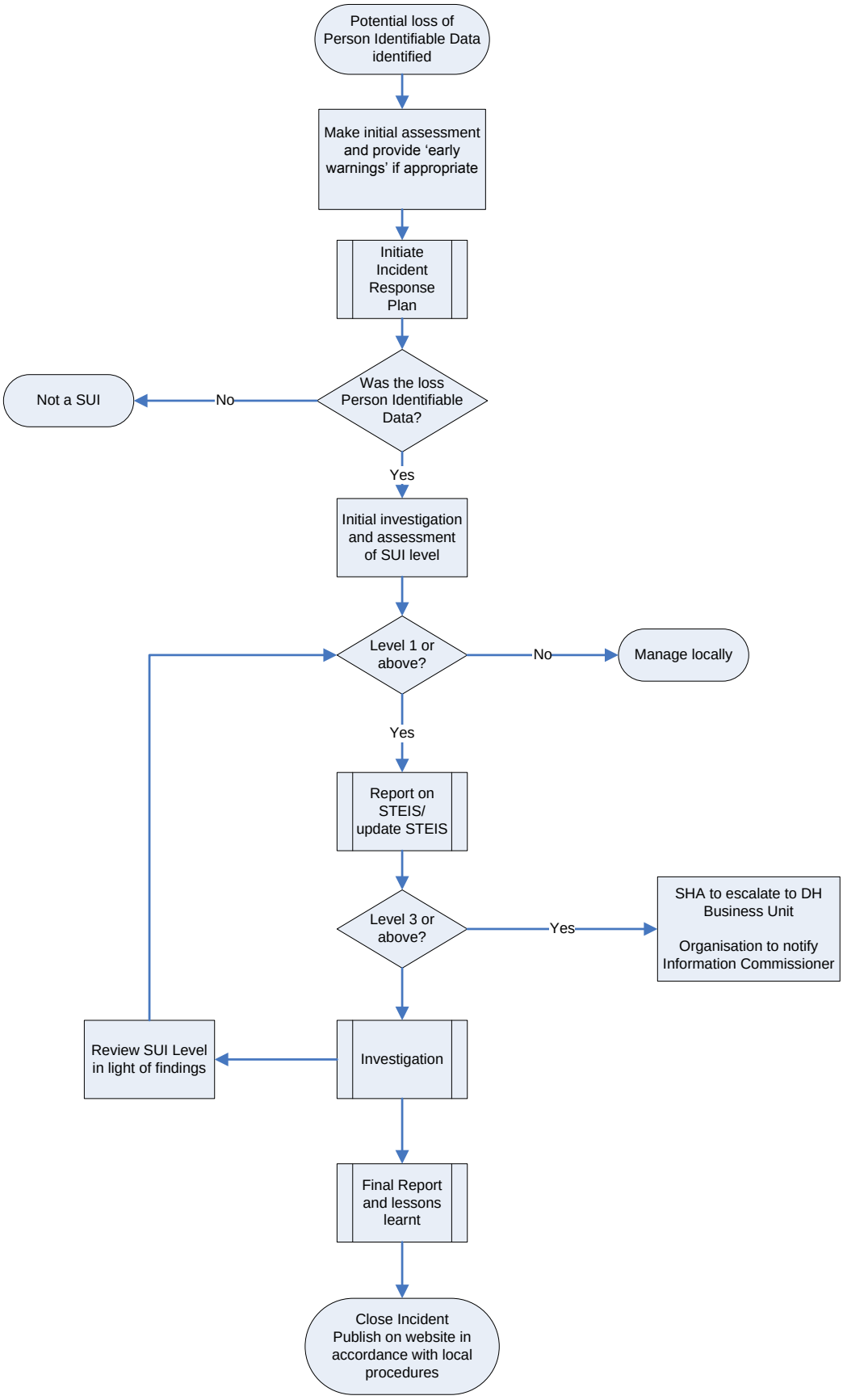
2.5 All organisations should already have in place an Incident Response Plan (IRP) covering Disaster Recovery, Business Continuity and the development of effective Communications Plans. It is recommended that this checklist is incorporated into the IRP.

2.6 PCTs will be responsible for performance managing the investigation of SUIs in their main providers. Where the SUI takes place in a PCT, the SHA performance lead will manage the investigation.

2.7 The main parts of the process are:

- Initial reporting
- Managing the incident
- Investigating
- Final reporting

IG SUI Management Process – High level view



3. Initial Reporting of Serious Untoward Incidents

3.1 Suspected incidents

Initial information is often sparse and it may be uncertain whether a SUI has actually taken place. Suspected incidents and 'near misses' should be reported as SUIs as lessons can often be learnt from them and they can be closed when the full facts are known.

3.2 Early notification

Where it is suspected that an IG SUI has taken place, it is good practice to informally notify key staff (Chief Executive, Senior Information Risk Owner, Caldicott Guardian, other Directors, PCT, SHA, DH, etc.) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'. Each organisation needs to determine its own notification priorities.

3.3 Reporting incidents – STEIS will be used for reporting all SUIs and an initial report should be made as soon as possible and no later than 24 hours of the incident or first becoming aware of the incident. Further information will become available as the investigation takes place and STEIS should be regularly updated as appropriate.

3.4 The SHA monitors STEIS and will therefore be aware of all IG SUIs (although please note 3.2 concerning early notification).

3.5 Complete the information required for STEIS.

Ensure that the following are included in the report:

- Date, time and location of the incident
- Type of Incident: "Confidential Information Leak" (NB this may be subject to change as improvements to STEIS data incident reporting are being pursued)
- Contact details for local incident manager
- Confirmation that appropriate and documented incident management procedures are being followed and that disciplinary action will be invoked where appropriate following the investigation
- Description of what happened
    - Theft, accidental loss, inappropriate disclosure, procedural failure etc.
    - The number of patients/ staff (individual data subjects) involved
    - The number of records involved
    - The media (paper, electronic) of the records
    - If electronic media, whether encrypted or not
    - The type of record or data involved and sensitivity

- Whether the SUI is in the public domain
- Whether the media (press etc.) are involved or there is a potential for media interest
- Whether the SUI could damage the reputation of an individual, a work-team, an organisation or the NHS as a whole
- Whether there are legal implications for the trust
- Initial assessment of level of SUI (see table at Annex A and 4.2 “Assessing the Incident Level”).
- Whether the following have been notified (formally or informally):
    - Data subjects
    - Caldicott Guardian
    - Senior Information Risk Owner
    - Chief Executive
    - Accounting Officer
    - Information Commissioner for SUI level 3 and above
    - Police, Counter Fraud Branch, etc
    - PCT
    - SHA

- Immediate action taken, including whether any staff have been suspended pending the results of the investigation
- Whether the incident is externally reportable: for IG SUIs level 3 and above, local organisations should inform the Information Commissioner once the initial facts are known. The SHA will escalate to DH NHS Business Unit and Media Handling teams. The information that will be needed by the DH is provided in checklist form at Annex B.

4 Managing the incident

- Identify who is responsible for managing the incident and coordinating separate but related incidents
- Identify who is responsible for the investigation and performance management
- Identify expected outcomes
- Identify stakeholders
- Develop and implement an appropriate communications plan
- Preserve evidence
- Investigate the incident (below)
- Institute formal documentation – this must incorporate version control and configuration management
- Maintain an audit trail of events and evidence supporting decisions taken during the incident
- Where appropriate inform the Information Commissioner (SUI level 3 and above)

- Escalate as appropriate (PCT, SHA, SHA to DH Business Unit)
- Inform data subjects (patients, staff)
- Identify and manage consequent risks of the incident (these may be IG-related or involve risks to patient safety, continuity of treatment etc.)
- Identify and manage consequent risks of the incident (these may be IG-related or involve risks to patient safety or continuity of treatment etc.)
- Institute recovery actions
- Invoke organisation's disciplinary procedure as appropriate and document the reasons where it is decided not to take action where such action may be viewed as relevant by external parties
- Institute appropriate counter-measures to prevent recurrence
- Identify risks and issues that, whilst not 'in scope' of the incident, are appropriate for separate follow-up and action

4 Investigating the incident

4.1 Note that national guidance / requirements are expected on forensic preservation of evidence relating to IG incidents

- Appoint investigating officer
- Engage appropriate specialist help (IG, IT, Security, Records Management)
- Where across organisational boundaries coordinate investigations (and incident management)
- Investigate – carry out a Root Cause Analysis as per the NPSA's template using the Incident Decision Tree (NPSA tools are available on www.npsa.nhs.uk go to tools. All templates are downloadable. IDT, RCA and report writing and although they need a small of flexibility in order to reflect IG rather than patient safety issues they provide a good structure for investigating and reporting IG incidents).

  http://www.npsa.nhs.uk/nrls/improvingpatientsafety/patient-safety-tools-and-guidance/rootcauseanalysis/rca-investigation-report-tools/
- Organisations should be aware of rules of evidence, interviews, preservation of evidence, suspending staff, etc
- Document investigation and findings
- Ensure that content is reviewed with sources for accuracy
- Identify lessons learnt

4.2 Assessing the incident level

Although the primary factors for assessing the severity level are the numbers of individual data subjects affected, the potential for media interest, and the potential for reputational damage, other factors may indicate that a higher rating is warranted, for example the potential for litigation or significant distress or damage to the data subject(s). As more information becomes available, the SUI level should be re-assessed.

Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case should inform the assessment of the SUI level. When more accurate information is determined the level should be revised as quickly as possible and all key bodies notified.

Where the level of likely media interest is initially assessed as minor but this assessment changes due to circumstances (e.g. a relevant FOI request or specific journalistic interest) the SUI level should be revised as quickly as possible and all key bodies notified. Note that informing data subjects is likely to put an incident into the public/media domain.

5. Final Reporting and Closure of the incident

- Set target timescale for completing investigation and finalising reports
- Produce report as per NPSA template
- Report reviewed by appropriate persons or appraisal group.
- Sign-off of report – Investigating Officer and CE if serious enough
- Send to the relevant persons and/ or committee.
- Identify who is responsible for disseminating lessons learnt
- Closure of SUI – only when all aspects, including any disciplinary action taken against staff, are settled.
- Update STEIS
- Where the SUI has been escalated to DH Business Unit notify them, of the closure.
- Log SUI details for incorporation in end of year reports by Accountable Officer (see Annex C)
- Publish on Trust/ SHA website as appropriate

Annex A

DoH Guidance 20th Feb 2008 Gateway 9571.

1. Purpose of This Document

It is essential that all serious untoward incidents that occur in Trusts are reported appropriately and handled effectively. This document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when a serious untoward incident occurs. Trusts should ensure that any existing policies for dealing with Serious Untoward Incidents are updated to reflect these arrangements.

2. Definition of a Serious Untoward Incident in relation to Personal Identifiable Data

There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. As a guide, 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.

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

3. Immediate response to Serious Untoward Incident

Trusts should have robust policies in place to ensure that appropriate senior staff are notified immediately of all incidents involving data loss or breaches of confidentiality.

Where incidents occur out of hours, Trusts should have arrangements in place to ensure on-call Directors or other nominated individuals are informed of the incident and take action to inform the appropriate contacts.

4. Assessing the Severity of the Incident

The immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.

Risk assessment methods commonly categorise incidents according to the likely consequences, with the most serious being categorised as a 5, e.g. an incident should be categorised at the highest level that applies when considering the characteristics and risks of the incident.

0	1	2	3	4	5
No significant reflection on any individual or body Media interest very unlikely	Damage to an individuals 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.	Damage to an organisation's reputation/ Local media coverage.	Damage to NHS reputation/ National media coverage.
Minor breach of confidentiality. Only a 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 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

5. Reporting to the SHA

The Trust should report the SUI, i.e. all incidents rated as 1 – 5, to the SHA through the usual SUI process. The following information should be provided in each case:

- A short description of what happened, including the actions taken and whether the incident has been resolved
- Details of how the information was held: paper, memory stick, disc, laptop etc
- Details of any safeguards such as encryption that would mitigate risk
- Details of the number of individuals whose information is at risk
- Details of the type of information: demographic, clinical, bank details etc
- Whether a) the individuals concerned have been informed, b) a decision has been taken not to inform or c) this has not yet been decided
- Whether a) the Information Commissioner has been informed, b) a decision has been taken not to inform or c) this has not yet been decided
- Whether the SUI is in the public domain and the extent of any media interest and/or publication

Reporting to the SHA should be undertaken as soon as practically possible (and no later than 24 hours of the incident during the working week).

If there is any doubt as to whether or not an incident meets the SUI reporting criteria, the Trusts' Risk Manager or the SHA should be contacted by telephone for advice. Early information, no matter how brief, is better than full information that is too late.

The Trust should keep the SHA informed of any significant developments in internal/external investigations, as appropriate. The SHA should continue to keep a watching brief on developments including following up further details/outcomes of the incident.

The Trust's communications team should contact the SHA's Communications team immediately if there is the possibility of adverse media coverage in order to agree a media handling strategy. Where necessary, the SHA Communications team will brief the Department of Health Media Centre.

6. Reporting to the Department of Health

The SHA will be responsible for notifying the DH of any category 3-5 incident reported by forwarding details to the appropriate dedicated mailbox established within the DH. Incidents should be notified to DH comms only if only the lighter shaded risk areas in the top two rows in the table apply, and to both DH Comms and the NHS Business Unit if the significant risks in the darker shaded area at the bottom right of the table apply. This latter, most serious category, is the one that should be referenced as a nationally reported SUI. Those reported to DH Comms alone should be referred to as a comms alert derived from a local SUI. Once an incident has been reported to DH any subsequent details that emerge relating to the investigation and resolution of the incident should also be supplied.

The DH will review the incident and determine the need to brief Ministers and/or take other action at a national level.

7. Reporting to the Information Commissioner or other Bodies.

The Information Commissioner should be informed of all Category 3-5 incidents. The decision to inform any other bodies will also be taken, dependent upon the

circumstances of the incident, e.g. where this involves risks to the personal safety of patients, the National Patient Safety Agency (NPSA) may also need to be informed.

8. Informing Patients

Consideration should always be given to informing patients when person identifiable information about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this done.

Annex B

Information required by the Department of Health for category 3+ SUIs

Unique SUI Reference:		
Initial assessment of level of SUI (1-5):		
SHA Responsible:		
Local Organisation(s) involved:		
	Required Information	**Check**
01	Date, time and location of the incident	
02	Confirmation that DH guidelines for incident management are being followed and that disciplinary action will be invoked if appropriate	
03	Description of what happened: Theft, accidental loss, inappropriate disclosure, procedural failure etc.	
04	The number of patients/ staff (individual data subjects) data involved and/or the number of records	
05	The type of record or data involved and sensitivity	
06	The media (paper, electronic, tape) of the records	
07	If electronic media, whether encrypted or not	
08	Whether the SUI is in the public domain and whether the media (press etc.) are involved or there is a potential for media interest	
09	Whether the reputation of an individual, team, an organisation or the NHS as a whole is at risk and whether there are legal implications	
10	Whether the Information Commissioner has been or will be notified and if not why not	
11	Whether the data subjects have been or will be notified and if not why not	
12	Whether the police have been involved	
13	Immediate action taken, including whether any staff have been suspended pending the results of the investigation	
14	Whether there are any consequent risks of the incident (e.g. patient safety, continuity of treatment etc.) and how these will be managed	
15	What steps have been or will be taken to recover records/data (if applicable)	
16	What lessons have been learned from the incident and how will recurrence be prevented	
17	Whether, and to what degree, any member of staff has been disciplined – if not appropriate why?	
18	Closure of SUI – only when all aspects, including any disciplinary action taken against staff, are settled.	
Notes:		

Annex C

Publishing details of SUIs in annual reports and Statements of Internal Control

Principles

The reporting of personal data related incidents in the Annual Report should observe the principles listed below. The principles support consistency in reporting standards across Organisations while allowing for existing commitments in individual cases.

a) You must ensure that information provided on personal data related incidents is complete, reliable and accurate.
b) You should review all public statements you have made, particularly in response to requests under the Freedom of Information Act 2000, to ensure that coverage of personal data related incidents in your report is consistent with any assurances given.
c) You should consider whether the exemptions in the Freedom of Information Act 2000 or any other UK information legislation apply to any details of a reported incident **or** whether the incident is unsuitable for inclusion in the report for any other reason (for example, the incident is *sub judice* and therefore cannot be reported publicly pending the outcome of legal proceedings).
d) Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Untoward Incident unless you have reason to believe that the protections have been broken or were improperly applied.

Content to be included in Annual Reports

Incidents classified at a severity rating of 3-5 (see Annex A) are those that should be captured as Serious Untoward Incidents and should be reported to SHAs and to the Information Commissioner. These incidents need to be detailed individually in the annual report in the format provided as Table 1 below. All reported incidents relating to the period in question should be reported, not just those that have been closed.

Table 1

SUMMARY OF SERIOUS UNTOWARD INCIDENTS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONER'S OFFICE IN 2007-08				
Date of incident (month)	**Nature of incident**	**Nature of data involved**	**Number of people potentially affected**	**Notification steps**
Jan	Loss of inadequately protected electronic storage device	Name; address; NHS No	1,500	Individuals notified by post
Further action on information risk	The [organisation] will continue to monitor and assess its information risks, in light of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems. The member of staff responsible for this incident has been dismissed.			

Notes to producing Table 1
Nature of the incident *Select one of :* a) Loss of (*insert from category list below*) from secured NHS premises b) Theft of (*insert from category list below*) from secured NHS premises c) Loss of (*insert from category list below*) from outside secured NHS premises *(including, for example, post, courier, loss by a contractor or third party supplier)* d) Theft of (*insert from category list below*) from outside secured NHS premises *(including, for example, theft from employee home or car* e) Insecure disposal of (*insert from category list below*) *(including, for example, sale of computers with unwiped hard drives, disposal of unshredded paper documents)* f) Unauthorised disclosure *(including, for example, criminal, negligent or inappropriate use of an information system or information asset by a staff member, contractor or third party supplier, resulting in disclosure; disclosure as a result of software or systems failure)* g) Other
Category List i) inadequately protected PC(s), laptop(s) and remote device(s) *(including, for example, PDAs, mobile telephones, Blackberrys)* ii. inadequately protected electronic storage device(s) *(including, for example, USB devices, discs, CD ROM, microfilm)* iii. inadequately protected electronic back-up device(s) *(including, for example, tapes)* iv. paper document(s)
Nature of data involved *A list of data elements (e.g. name, address, NHS number).*
Number of people potentially affected *An estimate should be provided if no precise figure can be given.*
Notification steps Individuals notified by post* / email* / telephone* (**delete as appropriate*) Police* / law enforcement agencies* notified (**delete as appropriate*) Media release
Further action on information risk A summary of any disciplinary action taken as a result of the incidents should also be included.

Incidents classified at lower severity ratings

Incidents classified at a severity rating of 1-2 should be aggregated and reported in the annual report in the format provided as Table 2 below.

Incidents rated at a severity rating of 0 need not be reflected in annual reports.

Table 2

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN 2007-08		
Category	**Nature of incident**	**Total**
I	Loss/theft of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	
II	Loss/theft of inadequately protected electronic equipment, devices or paper documents from outside secured NHS premises	
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	
IV	Unauthorised disclosure	
V	Other	

SIC Guidance

It is important to remember that an organisation's assets include information as well as more tangible parts of the estate. Information may have limited financial value on the balance sheet but it must be managed appropriately and securely. All information used for operational purposes and financial reporting purposes needs to be encompassed and evidence maintained of effective information governance processes and procedures with risk based and proportionate safeguards. Personal and other sensitive information clearly require particularly strong safeguards. The Accountable Officer and the board need comprehensive and reliable assurance from managers, internal audit and other assurance providers that appropriate controls are in place and that risks, including information and reporting risks, are being managed effectively.

The SIC should, in the description of the risk and control framework, explicitly include how risks to information are being managed and controlled as part of this process. This can be done for example by referencing specific work undertaken by your organisation and by reference to your organisation's use of the Information Governance Toolkit. The SIC will then be reflected formally in your Annual report.

Any incidence of a Serious Untoward Incident (as described in Annex A) should be reported in the SIC as a significant control issue. For the avoidance of doubt these are those incidents with a severity rating of 3,4 or 5.