There are documented information security incident / event reporting and management procedures that are accessible to all staff

**Requirement No:** 13-302  
**Initiative:** Information Security Assurance  
**Organisation Type:** Acute Trust  
**Version:** 13.0

**Requirement Description**

Damage resulting from potential and actual Serious Incidents Requiring Investigation (SIRIs) and information security events should be minimised and lessons learnt from them. All security incidents, suspected or observed, should be reported, recorded and investigated and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur. This includes weaknesses identified in systems design or operational procedures that potentially may result in an information security incident.

**Information Security Assurance, Incident Management, Investigation and Reporting**

**Introduction**

1. ISO/IEC 27035 - Information technology — Security techniques — Information security incident management defines an *information security event* as “an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation which may be security relevant.” Not all security events will be security incidents, as investigation of some will establish that they pose no threat. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Any breach of legislation or best practice guidance should also be considered an incident and treated accordingly. The processing of personal data without a legal basis, where one is required, must be reported to the Board (or equivalent) and dealt with as a data breach e.g. ‘disclosed in error’. **Note** that breach-type categories are defined in the HSCIC checklist guidance discussed in paragraph 5 below.

2. Some incidents may be classified as Information Governance Serious Incident Requiring Investigation (SIRI). An IG SIRI is any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1998 and/or the Common Law of Confidentiality. This includes unlawful disclosure or misuse...
of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people’s privacy. This definition applies irrespective of the media involved and includes both electronic media and paper records relating to staff and service users.

3. Since June 2013 all NHS organisations processing health and adult social care personal data must use the IG Toolkit Incident Reporting Tool to report level 2 IG Serious Incidents Requiring Investigation (SIRI) to the Department of Health (DH), NHS England and the Information Commissioner’s Office (ICO). IG SIRI functionality will be extended in early 2015 to enable capture of cyber related incidents.

4. A cyber-related incident is anything that could compromise information assets within cyberspace. “Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.” Source: UK Cyber Security Strategy, 2011.

5. Further detail on the current process, assessing the severity of incidents, severity levels which are reportable to National Bodies etc. can be found within the latest HSCIC/DH ‘Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation’ (see the Knowledge Base Resources). This document also offers guidance on managing, investigating and publishing incidents.

**Reviewing Weakness and Threats**

6. A weakness exists where a previously unknown threat is identified that has not been addressed through normal risk analysis and management processes, e.g. a computer system may be vulnerable to new malicious code, or a change of building use results in the potential for new threats. Both incidents and weaknesses are considered events and are of concern for their potential to affect the confidentiality, integrity and availability of information. If you experience any issues with your system/service, please log this directly with your system supplier.

7. All events / incidents / weaknesses should be reviewed to determine the threat (potential or actual) so that they can be recorded and managed in accordance with correct procedure. The assessment must also include whether the recorded event / incident is considered to be an IG Serious Incident Requiring Investigation because if so, it must be escalated and treated in accordance with HSCIC/DH guidance described above.

8. Information security events are not always apparent, e.g. virus/malware attacks may not be detected by users, or a lost or stolen computer may be reported to Estates security staff or IT helpdesk, with the issues around information security not being realised. In this scenario, the potential impacts on sensitive information, including that relating to service users, stored on the computer may not be considered by the reporting department.

9. It is imperative, therefore, that a unified reporting scheme is implemented and maintained. Such schemes should involve the Information Risk Lead, and relevant Information Asset Administrators including; Information Security Manager, Risk Manager, Estates Security, Data Protection Officer, IG Manager / Officer, Communications staff, Human Resources staff, the *Caldicott Guardian* and where
necessary the Commissioner(s). In the case of 3rd party support organisations, these will also need to be involved, as they may be responsible for some aspects of IG/security practice.

Management of Information Security Incidents/Events

10. The Board (or equivalent) has overall responsibility for Information Governance compliance and therefore should ensure that adequate Information Governance measures are in place and reviewed e.g. policies, procedures, training and awareness. These measures include robust information security incident/event reporting.

11. The organisation should ensure that responsibility for managing information security incidents/events is documented within the IG Lead/SIRO/IAO (or equivalent) and other relevant job descriptions. Responsibilities should also be clearly explained in any contract or agreements with other organisations affected. This should include responsibilities for developing / reviewing procedures for detecting and responding to information security incidents/events and for reporting to and liaising with the IG Lead, SIRO, IAO and Caldicott Guardian (or their equivalents) on all events involving person identifiable information.

12. In cases where there is a breach of confidential personal data, the data controller, individual or organisation legally responsible for the data, should give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached.

Documented Information Security Incident/Event Reporting and Investigation Procedures

13. To deal with all eventualities, the organisation should ensure that it has a formal and accessible system in place for recording, reporting, investigating and resolving information security incidents/events. The specific requirements for reporting IG and Cyber Security Serious Incidents Requiring Investigation (SIRIs) as defined in HSCIC/DH guidance must also be followed.

14. Information security incidents/events may be detected by a person noticing something that gives cause for concern, whether technical, physical or procedure related. Whatever the source of the detection of an incident/event, the person who detected it is responsible for initiating the detection and reporting process/system. This could be any member of an organisation’s personnel, whether permanent or contracted. Therefore, appropriate and documented incident management procedures need to be in place so that staff know what to do.

15. An audit trail of incidents/events and evidence should support the decisions taken during an incident and assist the investigation process. Following an investigation, it is possible that an organisation’s disciplinary procedures may be invoked. If these procedures are invoked against a member of staff then the reasoning behind any decisions of disciplinary action taken need to be carefully documented. Where it has been decided not to take such action, those decisions will need to be substantiated as relevant external parties may wish to view them.

16. The incident management system does not need to be solely concerned with information security incidents/events: an organisational-wide reporting/management system which covers staff and service user safety, security and information breaches may be suitable as long as it incorporates Information Governance
events / incidents which are properly categorised, referenced and their outcomes identifiable in line with HSCIC guidance. For example, if the corporate system rates the severity of an incident using a different grading to the IG toolkit incident reporting tool/guidance then a mapping of the system grading should be carried out to ensure staff understand which IG incidents would meet DH Policy/ICO criteria for reporting (see the HSCIC/DH “Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation’ in the Knowledge Base Resources for detail on the criteria for assessing the severity of an IG or cyber security SIRI.

17. Many organisations may have a generic incident reporting form that has initially been designed to report personal injuries, attacks, accidents and clinical incidents. Such reports are typically sent to the Risk Manager, rather than Information Security or IG Manager / Officers. Where this is the case, it is essential that such forms may also allow for the reporting of Information Security incidents and that both Risk and IG/Security managers liaise and are fully aware of their roles and procedures.

18. In many organisations the IT helpdesk will normally be informed of major and minor computer-related information security events. Modern helpdesk software allows the Information Security Manager / Officer to identify and analyse event patterns and potential threats. Extensive use should be made of this functionality where available and local helpdesk staff briefed to contact the responsible officer following suspected serious or widespread incidents.

19. It is essential that all users know who to report software malfunctions to (in larger organisations, this is normally the IT helpdesk) and that the Information Security Manager / Officer and IT staff liaise to identify and rectify common faults. Similar but remote helpdesk arrangements will also normally apply for those digital services provided to the organisation under commercial contract or other service agreement.

20. Other events, which are not computer-related, such as theft, loss or damage of paper-based files, fraud, may be reported to other departments, such as Estates, clinical risk, etc as appropriate. Therefore, it is essential that a reliable mechanism is in place to inform the Information Security/IG Manager / Officer in order that a holistic view of such events is obtained.

21. Investigation procedures and forensic capabilities (an organisation’s ability to investigate computer equipment usage retrospectively, without compromising the integrity of any evidence) should be developed to take account of the range of events that may occur. Some will be discrete procedures, such as investigating potential computer misuse (unauthorised or illegal data exchange and storage, fraud etc) and others will form part of Business Continuity Plans (see requirement 309). All such procedures will need to be developed in liaison with appropriate colleagues. Any investigations into incidents that are considered to be potential criminal activity should be treated extremely carefully to ensure that forensic investigations are not compromised in any way. External expert advice should be sought where there are any uncertainties with this.

22. An ‘Incident Management Plan’ is a ‘clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process. The incident management and response procedures should detail:

a. The need for the procedure.
b. The scope of the procedure.

c. An explanation of the types of incident, how they will be investigated and reported and any countermeasures.

d. Responsibilities of management and staff towards incident reporting.

e. Referenced documentation (e.g. the organisation’s Information Security Policy and Information Risk Policy).

f. For NHS organisations - current NHS and national guidelines.

g. Escalation arrangements involving others, including services and support providers who may also have involvement.

23. No matter how good existing procedures are, weaknesses will always become apparent. New threats and new systems or ways of working will expose these weaknesses and users on the ground are normally the first to identify them. Therefore, staff should be encouraged to report anything they feel threatens security, personal information or confidentiality. This approach needs to be adopted during induction training. Known but uncorrected weaknesses can lead to incidents.

Training and Awareness

24. It is essential that all personnel are made aware of and may easily access the procedures for reporting actual or suspected incidents/events that affect Information Governance. Induction training, annual refresher training and ad hoc training for particular departments/types of staff must all be considered to ensure personnel are aware of the procedures to follow. Event identification and reporting should be a core element of Information Governance training, with contact details and procedures made available in all departments. The Information Governance/Security Manager / Officer should ensure that reports are investigated and lessons fed back in future training or where appropriate to the staff concerned to encourage further participation and demonstrate the value of reporting to the organisation. Reports and recommendations should be made to the Information Risk Lead(s) (in NHS Trusts this will be the SIRO, IAO and Information Governance group or its equivalent).

25. Third party contractors and others (e.g. business partners, including other public sector bodies, the 'Charities, Social Enterprises and Voluntary Sector', commercial/external providers and Any Qualified Providers, commercial service providers etc), who may potentially use the organisation’s facilities should also be made aware of the importance of reporting perceived or actual incidents/events in line with the terms and conditions of service provision. In many cases it will not be possible for contractors and others to attend structured training / awareness events. Therefore, arrangements should be in place to provide affected individuals with copies of expected procedures.

26. Procedures for users to report incidents/events should include the following elements:

a. Definition of an incident/event.

b. Who, when, how and why incidents/events need to be reported.

c. Guidance to assess the impact and severity of the incident/event.
27. A variety of media can be used to help raise awareness and familiarise users with incident/event reporting, issues and consequences e.g.:
   a. Circulating the procedures to departments, with any explanatory notes.
   b. Advising staff of the procedure in a newsletter.
   c. Using handouts, leaflets or posters.
   d. At a training session or workshop.
   e. Using an intranet/internet site.

28. Materials and communication methods should be subject to regular review.

   **Please note:** it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

---

**Knowledge Base Resources**

<table>
<thead>
<tr>
<th>Title</th>
<th>Details</th>
<th>Last Reviewed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSCIC: Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (PDF, 445 KB)</td>
<td>This guidance document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when an IG or cyber security SIRI occurs. Organisations should ensure that any existing policies for dealing with IG and cyber security SIRIs are updated to reflect these arrangements.</td>
<td>27/02/2015</td>
</tr>
<tr>
<td>HSCIC: Information Governance Toolkit Incident Reporting Tool Publication Statement (PDF, 62 KB)</td>
<td>The purpose of this statement is to inform IG Toolkit Users and members of the public of our intent to publish data on Serious Incidents Requiring Investigation (IG SIRI) self reported on the secure IG Toolkit Information Governance (IG) Incident Reporting Tool.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td><strong>DH: NHS IG - Information Risk Management - Good Practice Guide 2009</strong></td>
<td>This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on ‘Data Handling Procedures in Government’. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>National Patient Safety Agency: Tools</strong></td>
<td>Incident Detection Tree (IDT), Root Cause Analysis (RCA) and report writing. Although they need a small degree of flexibility in order to reflect IG rather than patient safety issues they provide a good structure for investigating and reporting IG incidents.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td><strong>BS ISO/IEC 27000 Series of Information Security Standards</strong></td>
<td>Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td><strong>The UK Cyber Security Strategy</strong></td>
<td>The Cyber Security Strategy sets out how the UK will support economic prosperity, protect national security and safeguard the public’s way of life by building a more trusted and resilient digital environment.</td>
<td>09/02/2015</td>
</tr>
</tbody>
</table>
# Exemplar Materials

<table>
<thead>
<tr>
<th>Title</th>
<th>Details</th>
<th>Last Reviewed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walton Centre: Incident Reporting Standard (PDF, 182 KB)</td>
<td>This standard covers two separate but closely related areas: incident reporting, and incident response. Incident management is a cyclical process that requires identification/reporting of incidents, investigations and resolution and learning to reduce the risk of recurrence.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td>Walton Centre: Incident Response Standard (Legal and Forensics) (PDF, 192 KB)</td>
<td>A detailed incident response process including steps to take if legal and/or forensic expertise is required.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td>Walton Centre: Incident Response Standard (Operational) (PDF, 77 KB)</td>
<td>Response process for logging and responding to operational incidents.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td>DH: NHS IG - Incident Log (DOC, 29 KB)</td>
<td>Incident log template.</td>
<td>24/01/2015</td>
</tr>
<tr>
<td>Example Job Description - Information Security Manager/Officer (DOC, 81 KB)</td>
<td>This document provides organisations with an exemplar document for use when determining the qualities, experience and knowledge needed for applicants to the post of Information Security officer.</td>
<td>24/01/2015</td>
</tr>
</tbody>
</table>

# Useful Websites

<table>
<thead>
<tr>
<th>Title</th>
<th>Details</th>
<th>Last Reviewed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27035:2011 'Information technology – Security techniques – Information security risk management'</td>
<td>ISO/IEC 27005:2011 provides a framework for implementing a risk management approach to managing threats to information security management systems. In this second edition, the framework outlined in ISO/IEC 27005 has been reviewed and updated to reflect the content of the risk management documents.</td>
<td>24/01/2015</td>
</tr>
</tbody>
</table>
Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **Introduction to Information Governance** - an introductory level module aimed at all NHS staff to inform them about good Information Governance.
- **Information Governance: Medical Secretaries** - an introductory level module on information governance matters tailored for medical secretaries.
- **Information Governance: The Beginner's Guide** - an introductory level module that explains the importance of information governance to staff who do not generally require access to personal information.
- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Health and Social Care Information Centre and organisation administrators.

The Tool is available at: [www.connectingforhealth.nhs.uk/igtrainingtool](http://www.connectingforhealth.nhs.uk/igtrainingtool).

Requirement Origins

- Protecting and Using Patient Information, Caldicott Management Audit point 15
- Security Incidents
- Protecting and Using Patient Information, Caldicott Management Audit point 16
- Security Monitoring

Changes

The following is a list of *material* changes since the last major version of this requirement:
• Added guidance on new functionality that enables cyber SIRIs to be reported via the IG Toolkit Incident Reporting Tool.
• Added guidance on reporting the processing of personal data without a legal basis, where one is required, to the Board.
• Added guidance on apologising for data breaches.
• New attainment level 2c regarding reporting level 2 IG and cyber security breaches using the IG and Cyber Security Incident Tool.
• New attainment level 3c regarding providing information and an apology to individuals whose confidentiality has been breached.
**Attainment Levels (Including Checklist)**

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

<table>
<thead>
<tr>
<th>0</th>
<th>There is insufficient evidence to attain Level 1.</th>
</tr>
</thead>
</table>
| 1 | There are documented and approved processes for reporting, investigating and managing information security incidents / events.
   
   a  There are documented procedures for reporting, investigating and managing information security events, including IG and Cyber Security Serious Incidents Requiring Investigation.
      
      **Evidence Required:**
      • Documented reporting, investigating and managing information security events procedures.

   **Notes/other evidence:**

   b  The procedures have been approved by the SIRO, and Board or delegated sub-group involving IAOs or equivalent personnel.
      
      **Evidence Required:**
      • IG Management Framework document (which includes the date the procedures were approved and the approving individual/group).

   **Notes/other evidence:**

| 2 | The information security event reporting and management procedures have been communicated to staff/relevant third parties.
   
   a  The procedures have been effectively communicated to staff and third parties working on behalf of or under contract to the organisation, including the importance of reporting information security events and near misses.
      
      **Evidence Required:**
      • Staff briefing and/or induction materials, and policies folder on computer desktops, or policies section of the local Intranet, or hard copies found in communal areas.

   **Notes/other evidence:**

   b  Contracts or agreements with service providers and business partner organisations have been reviewed to ensure these include clear reporting requirements, enforceable obligations, expectations and references to procedures for the reporting of and response to incidents.
      
      **Evidence Required:**
      • A list of contracts and the dates that they were reviewed and content approved.

   **Notes/other evidence:**
| c | Data breaches and cyber incidents reaching Level 2 (see HSCIC checklist guidance in the Knowledge Base Resources) are reported through the IG and Cyber Security SIRI Tool.  
**Evidence Required:**  
- Where a breach has occurred, copies of Serious Incidents Requiring Investigation reports.  
- If there have been no level 2 breaches, state this in the comments section or add the words ‘not relevant’.  
**Notes/other evidence:** |
| 3 | The SIRO and IAOs or equivalent, monitor compliance with the procedures, taking corrective action if evidence of non-compliance is discovered. Incidents are analysed and where necessary, systems and processes are refined to minimise the risk of recurrence.  
**a** | The SIRO and IAOs (or equivalent) monitor compliance with the security event reporting procedures and instigate remedial action where procedures have not been followed.  
**Evidence Required:**  
- Incident logs, analysis of reported security incidents and causes, improvement plans, lesson learned reports, results from staff surveys, spot check analysis or reports (e.g. NHS Statement of Internal Controls).  
**Notes/other evidence:** |
| **b** | Reported information security events are analysed and measures implemented to tackle common problems and root causes.  
**Evidence Required:**  
- Documented analysis of information security events with actions taken/suggested.  
- Formal reports produced for the SIRO (or equivalent) and Board (or equivalent) where incidents have occurred.  
**Notes/other evidence:** |
| **c** | Where there is a breach of confidential personal data, the individual whose confidentiality has been breached is provided with a full explanation of the cause and an apology, and of the remedial action being undertaken to prevent recurrence.  
**Evidence Required:**  
- Sample communications with people whose confidentiality has been breached, demonstrating that an explanation including an apology has been given.  
- If there have been no breaches of confidential personal data, state this in the comments section or add the words ‘not relevant’.  
**Notes/other evidence:** |
It is important that information security event reporting, control and investigation guidance / procedures, training and awareness measures are subject to regular review to ensure they remain effective.

**Evidence Required:**
- Minutes/meeting notes where the guidance / procedures, training and awareness measures have been reviewed including the decisions made and any updates.

**Notes/other evidence:**

<table>
<thead>
<tr>
<th>Past Level:</th>
<th>Current Level:</th>
<th>Target Level:</th>
<th>Target Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(available online from IGT)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>