NHS England

Information Security Incident Reporting Procedure

Information Security Incident Reporting Procedure

Version number: Draft 3.0

First published: 2013

Updated: June 2015

Prepared by: [redacted]

Contents

1 Introduction

1.1 Information security is everyone's responsibility; these procedures have been developed to assist the organisation's employees to identify information governance incidents, suspected information security weaknesses or near misses, information security threats to services or systems and how to report these incidents through appropriate management channels.

1.2 The NHS England centralised incident reporting tool has been developed. This guidance has therefore been developed to provide the arrangements for Information Governance (IG) incident management for NHS England, including Regional Teams, NHSIQ and Commissioning Support Units (CSU's).

2 Scope

2.1 The following staff of NHS England are in scope of this document

- National Support Centre Teams;
- Regional Teams;
- Commissioning Support Units;
- NHSIQ;
- Clinical Senates;
- Clinical Networks;
- Staff working in or on behalf of NHS England (this includes contractors, temporary staff, secondees and all permanent employees);
- Relevant contracted third parties.

2.2 Third party contractors for services being provided on behalf of NHS England must have incident reporting obligations written in to the contracts. The third party is obligated to report NHS England responsible incidents to the nominated NHS England local contact. The NHS England local contact is responsible for ensuring this Information Security Incident Reporting Procedure is followed.

2.3 All primary care independent contractors e.g. GP's, Dentists, Opticians and Pharmacists must have their own incident management procedure to follow and are therefore outside of this scope.

3 An Information Security Incident

3.1 An information governance incident is any violation of the organisation's IG Policies. The term security incident and suspected incidents is very broad and includes, but is not limited to, incidents that affect disclosure, denial of access to, destruction or modification of NHS England's data.

3.2 An incident may arise in any of the many information handling requirements, including;

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The NHS Confidentiality Code of Practice
- The Information Security Management NHS Code of Practice
- The Records Management NHS Code of Practice
- The NHS Information Governance Toolkit Requirements

3.3 Examples of security incidents:

- Using another user's login id
- Unauthorised disclosure of information
- Leaving confidential / sensitive information unsecure
- Theft of IT equipment
- Accessing a persons' record inappropriately e.g. viewing your own health record or family members, neighbours, friend etc,
- Sharing a smartcard
- Misuse of email / internet
- Installing unauthorised software
- Threat of cyber security

3.4 Diligent employees should question procedures, protocols and events that they consider could cause damage, harm, distress, breach of compliance or bring the organisations name into disrepute.

3.5 By reporting incidents it allows the organisation to relate to similar occurrences and highlights any areas of vulnerability, identifying where greater awareness is needed, or procedures/ protocols that require reviewing. Good reporting generates better statistical data thus, keeping the organisation informed.

3.6 All incidents will be reviewed by the relevant Region or Central Team IG Lead and monitored, to identify recurring or high impact incidents. This may indicate the need for enhanced or additional controls. When reporting an information security incident, it is important to ensure sufficient information is given to enable the Corporate Information Governance Team to understand and respond appropriately to the report.

3.7 If it is not clear if a possible incident requires reporting, the Region or Central Team IG Lead can provide advice if necessary.

4 Description of Incident

4.1 It is important that security incident reports provide as much detail as possible. These should include a description of activities leading up to the security incident, information about circumstances prevailing at the time, how the incident came about, how the security incident was detected.

4.2 The security incident or suspected security incident report where possible should not include personal identifiable information in the free text fields.

4.3 Whenever possible when reporting security incidents, relate them to the protocols or procedures that may have been compromised. An audit report can be a useful document, providing background to security incidents.

4.4 Security incidents must be reported as soon as possible after the event has been identified. Reports sent immediately after the incidents are likely to be the most valuable; if there is a delay between an incident occurring and the discovery of said incident, it should still be reported.

4.5 Whenever possible document in the incident report any immediate mitigation actions that have been taken.

5 Reporting of Information Security Incidents

5.1 All IG incidents that NHS England are responsible for should be reported utilising the IG incident electronic form via NHS England's Information Security Portal, within 24 hours of becoming aware of the incident.
The electronic form is located - https://nhsengland.sharepoint.com/TeamCentre/TCO/ICT/ITSecurity/Information%20Security%20Incident%20Portal

5.2 Commissioning Support Units (CSU's) or Primary Care Support Services Provider (PCSS) can utilise their own internal process / system for the recording of incidents, but must follow details of all Level 1 incidents as stated in 5.7.4 and follow the process in 5.8 for Level 2 and above incidents.

5.3 The incident must be graded for severity using the Health and Social Care Information Centre's (HSCIC) grading tool in the Checklist guidance for reporting, managing and investigating information governance serious incidents requiring investigation – Annex A), (Appendix 1).

5.4 An NHS England incident must be submitted utilising the electronic form, this will alert the Corporate IG Team via an email to the england.ig-corporate@nhs.net mailbox. Opening the incident electronic form will have generated its own unique reference number and this will be included in the alert email once submitted.

5.5 The email alert will be allocated to the relevant Region / Central Team IG Lead for reviewing and verification that the grading is appropriate, ensure the incident is being investigated appropriately and provide support if required and update and close the incident via the NHS England Information Security Portal.

5.6 The same incident form will also be used for the reporting of any IT security incidents identified and the IT security team will be alerted to these for further investigation and management.

5.7 Incidents graded Level 1 or below

5.7.1 Incidents graded as a Level 0 or below are considered a ‘near miss.

5.7.2 Incidents graded as a Level 1 or below are to be investigated and managed locally by the Region / Directorate responsible for the incident.

5.7.3 The responsible Region / Directorate must inform the relevant Region / Central Team IG Lead upon the conclusion of the investigation that the incident can be closed.

5.7.4 CSU’s / PCSS can utilise their own internal process / system for the management of these incidents. A log must be maintained and provided to the Corporate IG team for inclusion in the Central Team incident reports to the Central Team IG Group. The information will be requested from the Corporate IG Team on a quarterly ~~basis .~~ basis. (See Appendix 3)

5.8 Incidents graded Level 2 or above

5.8.1 The relevant Region / Central Team IG Lead will review the incident form and verify with the CSU / PCSS / Region /Directorate that the grading is appropriate.

5.8.2 The relevant Region / Central Team IG Lead to advise the Head of Corporate Information Governance to ensure the incident is reported through the Health and Social Care Information Centre (HSCIC) IG Toolkit SIRI reporting tool.

Once a level 2 incident is reported via the tool, a notification is immediately sent to the Department of Health and the Information Commissioner's Office.

5.8.3 The CSU / PCSS / Region / Central Team IG Lead must inform their Deputy Senior Information Risk Owner (SIRO) and relevant Caldicott Guardian as appropriate of the incident.

5.8.4 The incident should be managed in line with the HSCIC's Checklist guidance for reporting, managing and investigating information governance serious incidents requiring investigation – Section 5.2 - 5.5.

5.8.5 The Head of Corporate Information Governance will inform the NHS England SIRO and NHS England Caldicott Guardian.

5.8.6 A process diagram for Central Team / Regions is shown in Appendix 4.

5.8.7 A process diagram for CSU's / ~~PCSS is~~PCSS is shown in Appendix 5

6 Monitoring of Incidents

6.1 The Region / Central Team IG Lead is alerted to all IG incidents that are recorded and will monitor these incidents and discuss them with the relevant managers and staff.

6.2 The Region IG Lead / Central Team Lead will produce quarterly reports for the Region IG Group / Central Team IG Group.

6.3 The CSU / PCSS will provide the Central Team IG Lead with incident data on a quarterly basis to be included in the Central Team IG Group report.

6.4 The Corporate IG team will produce quarterly reports of all Level 2 incidents for the National IG Group. The Corporate IG team will produce regular lessons learnt bulletins.

7 Equality Impact Assessment

7.1 This document forms part of NHS England’s commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

7.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

Appendix 1 - IG SIRI Grading Tool

The following process should be followed to categorise an IG SIRI

Step 1: Establish the scale of the incident.
(If this is not known it will be necessary to estimate the maximum potential scale point.)

Scale Factors – Baseline Scale	
How many individuals are involved in the incident?	**Level**
Information about less than 10 individuals	**0**
Information about 11-100 individuals	**1**
Information about 101-1000 individuals	**2**
Information about 1,001 – 100,000+ individuals	**3**
Sensitivity Factors	
Step 2 : Identify which sensitivity characteristics may apply and the baseline score point to be adjust accordingly	
Low: For each of the following factors reduce the baseline score by 1	
(A) No sensitive personal data (as defined by the Data Protection Act 1998) at risk nor data to which a duty of confidence is owed	**-1**
(B) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000	**-1**
(C) Information unlikely to identify individual(s)	**-1**
High: For each of the following factors increase the baseline score by 1	
(D) Detailed information at risk e.g. clinical/care case notes, social care notes	**+1**
(E) High risk confidential information	**+1**
(F) One or more previous incidents of a similar type in the past 12 months	**+1**
(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information	**+1**
(H) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual	**+1**
(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment	**+1**
(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident	**+1**

Step 3:

Level 0: Incident categorised as a ‘near miss or non-event’ and to be investigated and managed locally.

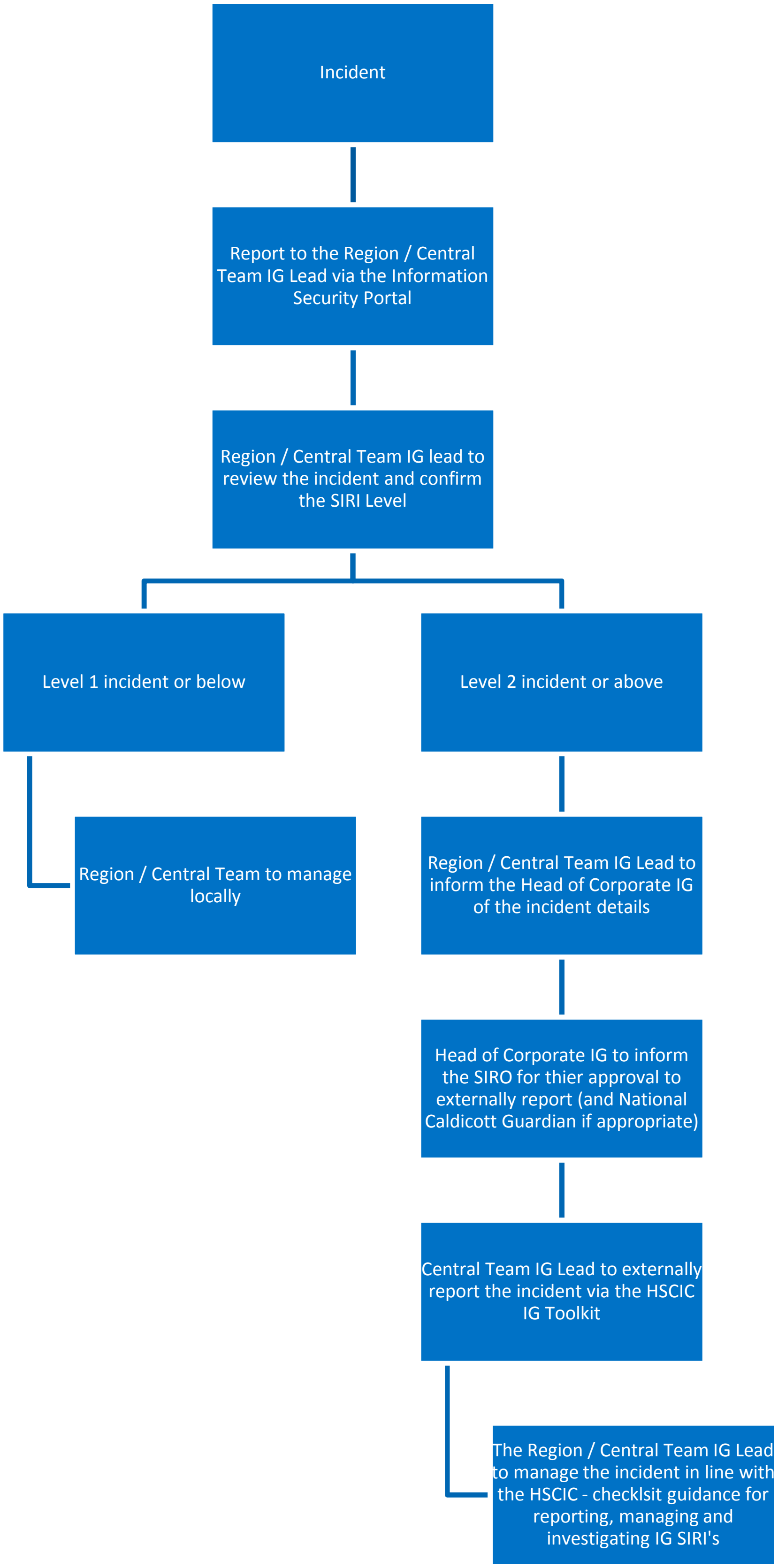
Level 1: Confirmed IG SIRI and to be investigated and managed locally, but no need to report to ICO, DH and other central bodies.

Level 2 or above: Confirmed IG SIRI that must be report to ICO, DH and other central bodies.

Appendix 2 – Quarterly Low Level Incident Data Reporting Template

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN Q1 - 2014-15		
Category	Breach Type	Total
A	Corruption or inability to recover electronic data	
B	Disclosed in Error	
C	Lost in Transit	
D	Lost or stolen hardware	
E	Lost or stolen paperwork	
F	Non-secure Disposal – hardware	
G	Non-secure Disposal – paperwork	
H	Uploaded to website in error	
I	Technical security failing (including hacking)	
J	Unauthorised access/disclosure	
K	Other	

Appendix 3 – Incident Reporting Flow Process for Central Team / Regions / Hosted Bodies (not CSU’s)



Incident

Report to the Region / Central Team IG Lead via the Information Security Portal

Region / Central Team IG lead to review the incident and confirm the SIRI Level

Level 1 incident or below

Region / Central Team to manage locally

Level 2 incident or above

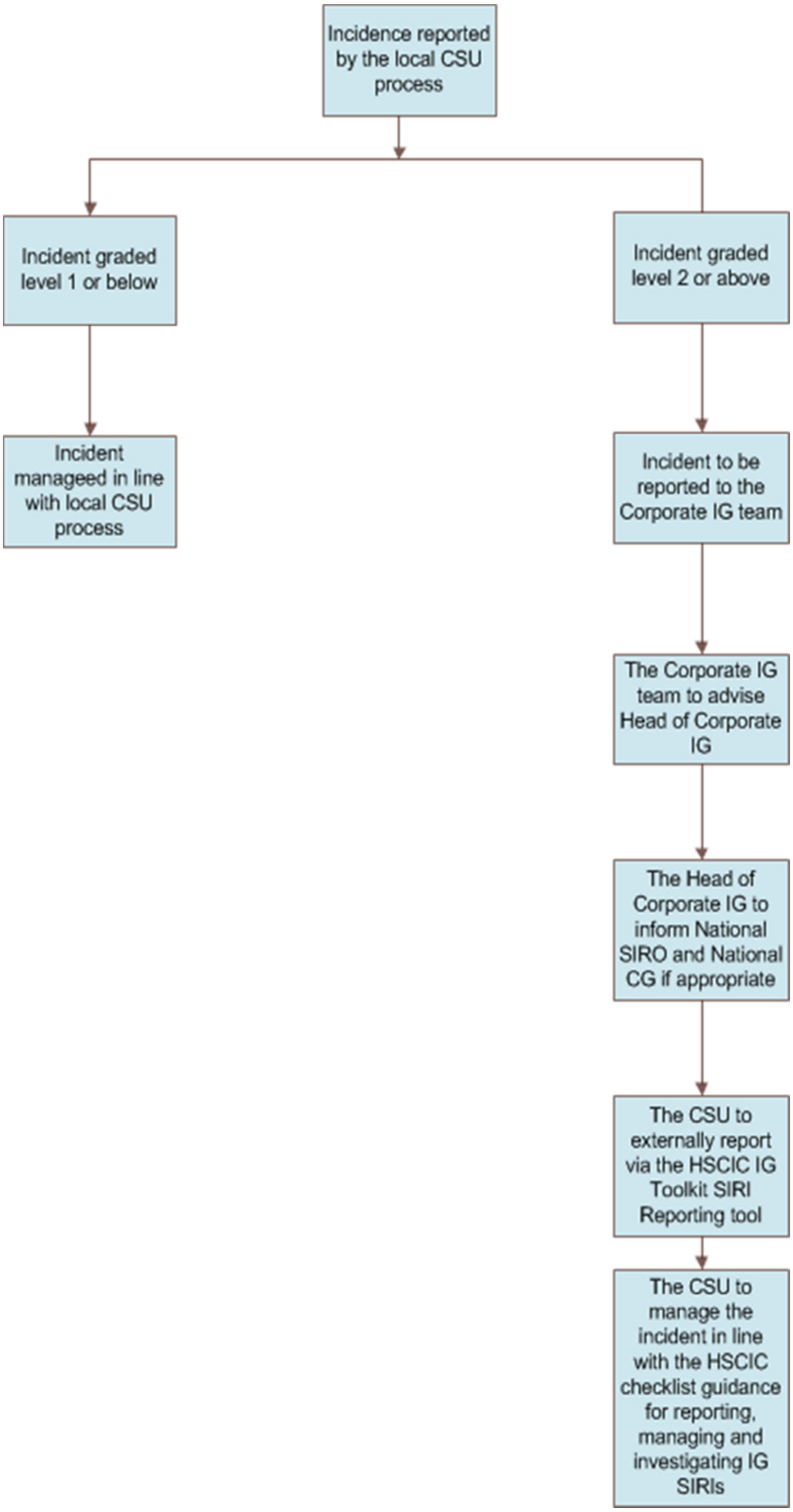
Region / Central Team IG Lead to inform the Head of Corporate IG of the incident details

Head of Corporate IG to inform the SIRO for thier approval to externally report (and National Caldicott Guardian if appropriate)

Central Team IG Lead to externally report the incident via the HSCIC IG Toolkit

The Region / Central Team IG Lead to manage the incident in line with the HSCIC - checklsit guidance for reporting, managing and investigating IG SIRI's

Appendix 5 – Incident Reporting Flow Process for CSU's / PCSS


Incidence reported by the local CSU process
Incident graded level 1 or below
Incident manageed in line with local CSU process
Incident graded level 2 or above
Incident to be reported to the Corporate IG team
The Corporate IG team to advise Head of Corporate IG
The Head of Corporate IG to inform National SIRO and National CG if appropriate
The CSU to externally report via the HSCIC IG Toolkit SIRI Reporting tool
The CSU to manage the incident in line with the HSCIC checklist guidance for reporting, managing and investigating IG SIRIs