North Hampshire
Clinical Commissioning Group

Information Incident Management and Reporting Procedures

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Version Control

Version	Date Issued	Details	Brief Summary of Change	Author
1.00	16/02/2014	Draft	New document	NHS South Commissioning Support Unit, Information Governance Team
1.10	19/03/2015	Final	Revised to reflect scoring amendments to HSCIC IG SIRI Incident Reporting Tool (07.11.2014).	NHS South Commissioning Support Unit, Information Governance Team
			Appendices 1, 2 & 3 updated to reflect NHCCG process and revised scoring guidance	D Broughall, Business Development Manager, NHCCG
1.20		Final	Organisational names and job roles updated. Revised to include reference to Cyber Security incidents	NHS South, Central & West CSU, Information Governance Team

For more information on the status of this policy, please contact:	
NHS South Commissioning Support Unit	Information Governance Team
Approved by	
Approval Date	
Next Review Date	
Responsibility for Review	Information Governance Team
Audience	All CCG officers and staff (which includes temporary staff, contractors and seconded staff) and CCG members in the capacity as commissioners.

Contents

Summary

North Hampshire Clinical Commissioning Group recognises the importance of reporting all incidents as an integral part of its risk identification and risk management strategy. The CCG is committed to improving the quality of service to patients/service users and the safety of staff and members of the public, through the consistent monitoring and review of incidents that result, or had the potential to result in confidentiality breach, damage or other loss.

Research has shown that the more incidents that are reported, the more information will be available about any problems. This allows action to be taken to make healthcare safer. The benefits of incident and near miss reporting include:

- Identifying trends across the organisation
- Pre-empting complaints
- Making sure areas of concern are acted upon
- Targeting resources more effectively
- Increasing awareness and responsiveness

The reporting and investigation of an incident forms part of a wider strategy for risk management, which advocates the use of root cause analysis to understand why an incident has occurred. The emphasis is upon critical exploration of the underlying and contributory factors, which if allowed to persist, could create the potential for the same error to be repeated again. Organisational learning and remedial action must be at the heart of any risk management approach.

Most information incidents relate to system failure and individual mistakes. Incident reporting needs an open and fair culture so that staff feel able to report problems without fear of reprisal and know how to resolve and learn from incidents.

The NHS recognises the importance of learning lessons from incidents. Through the introduction of standardised reporting and management arrangements the NHS wishes to ensure that where incidents occur in one organisation the lessons learnt are shared across all NHS organisations, key stakeholders and consumers of care.

1. Introduction

This document sets out how all incidents, including Serious Incidents Requiring Investigations (SIRIs), will be identified, reported by staff, and managed at the North Hampshire Clinical Commissioning Group (the CCG).

It is the responsibility of all staff to ensure that personal confidential data (PCD) remains secure and therefore, it is important to ensure that when incidents occur, damage from them is minimised and lessons are learnt from them.

The CCG is committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, permanent and temporary staff. This document is designed to achieve the following objectives:

- A standardised approach to incident management across the CCG;
- To ensure that learning from incidents is an integral part of the organisation's culture;
- Analysis of trends which may identify the further need for intervention;
- To improve staff patient/servicer users safety by addressing systematic errors;
- To promote a culture of accountability without 'blame'.

2. Aims and Objectives

The CCG will investigate and manage Information Governance and Cyber Security incidents including Serious Incident Requiring Investigations (SIRIs) and provide staff with guidelines on identifying and reporting information incidents including near-misses.

In doing so, the aim of the CCG is to promote a positive and non-punitive approach towards incident reporting, as long as there has been no flagrant disregard of the CCG's policies, fraud or gross misconduct. This document should be read in conjunction with other CCG related policies. (Please see section 11 for related CCG policies).

This document applies to incidents that impact on the security and confidentiality of personal information. Information incidents can be categorised by their effect on data subjects:

- Confidentiality e.g. unauthorised access, data loss or theft causing an actual or potential breach of confidentiality;
- Integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information;
- Availability, e.g. records are missing, misfiled, or have been stolen compromising or delaying patient care.

.

3. Definition of Terms Used

3.1 Incident

An Incident is defined as an event which has happened to, or occurred with, a patient(s), staff or visitor(s), the result of which might be harmful or potentially harmful, or which does cause or lead to injury/harm.

3.2 Serious Incident Requiring Investigations (SIRIs)

Serious Incident Requiring Investigations (SIRIs) are incidents which involve actual or potential failure to meet the requirements of the Data Protection Act 1998 and/or the Common Law Duty 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.

IG Cyber SIRI

A cyber- related incident is anything that could (or has) compromised 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 business, infrastructure and services." It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation for example, denial of service attacks, phishing emails and cyber bullying.

3.3 Adverse Event

Any untoward occurrence which can be unfavorable and an unintended outcome associated with an incident.

3.4 A Near Miss

A near miss is an incident that had the potential to cause harm but was prevented.
These include clinical and non-clinical incidents that did not lead to harm or injury, disclosure or misuse of confidential data but had the potential to do so.

4. Roles and Responsibilities

4.1 Accountable Officer

The Accountable Officer, has overall responsibility for information governance within the CCG. The AO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The AO has delegated operational responsibility for information governance to the Senior Information Risk Owner (SIRO).

4.2 Senior Information Risk Owner (SIRO)

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Chief Finance Officer. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the Governing Body and Finance & Performance Committee.

4.3 Caldicott Guardian

The role of CCG Caldicott Guardian has been assigned to the Chief Nurse who is a member of the Quality Committee with responsibilities for reflecting patients' interests regarding the use of Personal Confidential Data (PCD). The Caldicott Guardian will ensure that incidents, including unauthorised disclosure of confidential information are promptly reported to the Senior Information Risk Owner (SIRO) for consideration of any necessary actions.

4.4 NHS South, Central & West Commissioning Support Unit Information Governance Service Lead

The Head of Information Governance (IG) for NHS South, Central & West Commissioning Support Unit (SCW CSU(has been appointed to act as the overall Information Governance Lead for the CCG and under the approved arrangements, IG services will be provided by the IG Team of (SCW CSU) by way of a service specification.

The CSU Head of Information Governance is responsible for ensuring all tasks delegated to SCW CSU IG Team meet the required standards in line with the service specification.

4.5 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) should be senior members of staff at director/assistant director level or heads of department. They are responsible for providing assurance to the SIRO that information risks and incidents are identified and recorded, and that controls are in place to mitigate the risk or incident from occurring.

4.6 Data Custodians

Data Custodians should ensure that:

- All IG incidents are reported through the CCG's Risk Management Process within 24 hours of becoming aware.
- They consult with their IAO on incident management procedures and inform the CSU IG Manager of any breach;
- They familiarise themselves with the Health and Social Care Information Centre (HSCIC) guidance Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation;
- Recognise actual or potential incidents and take steps to mitigate the risks;
- Staff in their departments follow the CCG's procedures and guidance.

4.7 Managers and Supervisors

All managers, team leaders and supervisors (or deputy) are responsible for:

- Ensuring that all staff within their sphere of responsibility are familiar with this procedure and other IG policies and procedures
- Ensuring that all incidents within their sphere of responsibility are reported and recorded on the Incident Report systems (Datix).
- Monitoring incident reported on Datix for accuracy and completeness and taking steps to improve performance where omissions are identified.
- Ensuring SIRIs are brought to the immediate attention of the SIRO, Line Managers/Heads of Department (On-Call Manager out-of-hours).

All information incidents should be reported via the CCG incident reporting system (Datix) as soon as it is perceived that a breach has occurred. Incidents relating to confidentiality or data protection will be automatically copied to the Information Governance Manager and upon receipt.

Staff guidance on identifying and reporting information incidents can be found in Appendix 1 of this document.

5. Reporting, Managing and Investigating Information Incident

The Health and Social Care Information Centre (HSCIC) issued, a *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation* (May 2015).

The purpose for an incident investigation is to determine the facts concerning the incident and:

- To identify whether any deficiencies in the application of the CCG's policies or procedures and/or the CCG's arrangements for confidentiality and data protection contributed to the incident or;
- Determine whether a human error has occurred, but not to allocate blame;
- Establish what actually happened and what actions need to be taken to prevent reoccurrence.
- Carry out root cause analysis in order to ascertain the cause and to make recommendations

As part of an initial assessment of an incident, the SCW CSU's Head of IG/IG team will liaise with the directorate/department's IAO or line manager, Data Custodian, and the CCG's SIRO to ensure incidents are correctly graded and reviewed.

The SCW CSU's Head of IG, IG team and responsible IAOs and Data Custodians and will establish a process so that all facts are looked at and the investigation will be based on establishing what actually happened and what actions need to be taken to prevent

reoccurrence, **but not to allocate blame.** However, in some cases the investigation may identify whether any disciplinary processes may need to be invoked.

A root cause analysis investigation (RCA) may need to be created to allocate actions to various individuals and to ascertain the root cause of the incident.

The decision to notify a data subject (patient/service user) will be made by CCG's SIRO and the Caldicott Guardian on the grounds of disclosure, including transparency and the ability to protect against harm. This may include theft or blackmail; weighed against the potential harm that may be caused to the subject if notified of the incident.

Where an incident occurs out of business hours, the designated on-call officer will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident.

Please see appendix 2 of this document which outlines process for reporting and managing incidents (Flowchart).

5.1 Assessing the severity of an incident

The primary factors for assessing the severity level of incidents are determined by:

- The numbers of individual data subjects affected;
- sensitivity factors selected;
- the potential for media interest;
- the potential for reputational damage;

Other factors may indicate that a higher rating is necessary, for example the potential for litigation or significant distress or damage to the data subject and other personal data breaches of the Data Protection Act. As more information becomes available, the IG SIRI level will be re-assessed by the investigating team

Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case will inform the assessment of the SIRI level. When more accurate information is determined the level will be revised as quickly as possible.

5.2 Categorising Information Governance incidents including SIRIs

The categorisation of IG and Cyber Security incidents including SIRIs, is determined by the context, scale and sensitivity. An initial assessment of the incident will be made using the Health and Social Care Information Centre (HSCIC) 'Checklist Guidance for Reporting, Managing and Investigating SIRIs'.

Please see appendix 3 of this document that outlines procedure for assessing the severity of an incident and the categorisation process.

5.3 IG SIRI categorisation review

Incidents which have been categorised as potential level 2 or higher will be investigated and considered in greater detail and findings will be reported to the SIRO and Caldicott Guardian.

The decision to report a level 2 incident is the responsibility of the Senior Information Risk Owner (SIRO) together with the Caldicott Guardian. Once agreed the SCW CSU Head of IG/IG team will ensure that they are reported to the Department of Health (DH), Information Commissioners Office (ICO) and other regulators through the use of the IG Toolkit Incident Reporting Tool. Details of the findings will be recorded by the SCW CSU IG team within 24 hours of becoming aware of the incident.

All parties including DH and ICO whom may have been notified of the incident previously will be updated on the investigation outcome and lessons learnt.

5.4 Reporting to third parties

Where it is suspected that an IG SIRI has taken place, staff should ensure that the SIRO, Caldicott Guardian, directors and other key staff are immediately informed as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'.

5.5 Internal Reporting

Any information incident that takes place that is not recorded as a SIRI will be included in IG reports circulated to the IGC. These are primarily for awareness and to identify trends in minor incidents.

IG incident reports will be presented to the relevant committee/s through the SIRO in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

6. Freedom of Information Requests (FoI)

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management of incidents. Incidents will be defined and where appropriate kept confidential, underpinning the Caldicott principles and the regulations outlined in the Data Protection and Freedom of Information Acts.

Non-confidential incidents relating to the CCG and their services will be available to the public through a variety of means including Governing Body reports and minutes and the procedures established to meet requirements in the Freedom of Information Act 2000. The CCG will follow established procedures to deal with queries from members of the public

7. Action Plans and Audit

The CCG will ensure that:

- There is continuous improvement in confidentiality and data protection and learning outcomes;
- All incidents are audited to ensure any recommendation made have been implemented;
- Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring;

This will ensure that the CCG fully embeds improvements to its information governance structure and demonstrate it is proactive in assessing and preventing information risk.

8. Record keeping

A record of all decisions, actions, and recommendations should be kept throughout the investigation and final report. The department's IAO, Data Custodian, SCW CSU Head of IG and IG team will ensure that:

- All records and documentation are kept in a secure location;
- Any Personal Confidential Data (PCD) including medical records, photos or other; evidence is secured at the start of the investigation;
  Records are kept in a logical order;
- File notes with dates are kept of all discussions; minutes of all meetings are produced.

9. Procedure Review

In line with the organisation's key documents, this document will be reviewed no later than 2 years from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review.

10. Dissemination and implementation

This procedure will be published on the intranet. IAOs and other senior managers are required to ensure that their staff understand its application to their practice.

Awareness of any new content or change in process will be through electronic channels e.g. through email, in staff bulletins etc. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the CSU Information Governance team.

11. Related documents policies and procedures

The following documentation relates to the management of information and together underpins the CCG's Information Governance Framework. This procedure should be read in conjunction with the following policies:

- Information Governance Policy

- Confidentiality and Data Protection Policy
- Records Management Policy
- Information Security Policy

12. Equality, diversity and mental capacity

The CCG recognises the diversity of the local community and those in its employment. The organisations aim to provide a safe environment free from discrimination and, a place where all individuals are treated fairly, with dignity and appropriately to their need.

This document was assessed against the SCW CSU Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time.

This document has been assessed and meets the requirements of the Mental Capacity Act 2005.

Appendix 1: Staff Guideline on Identifying and Reporting an Information Incident

This guideline applies to all staff including permanent, temporary and contract staff. All incidents must be reported to your line manager, Information Asset Owners, Data Custodians or the SCW CSU Information Governance team within 24 hours of becoming aware of the incident.

What should you report?

Here are some examples of information incidents that should be reported:

- Finding a computer printout of Personal Confidential Data (PCD) details laying around;
- Identifying that a fax that was thought to have been sent to a recipient had been received by an unknown recipient or organisation;
- Finding confidential waste in a 'normal' waste bin;
- Losing a mobile computing device with personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password;
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area;
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus;
- Sending a sensitive e-mail to an unintended recipient or 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation.

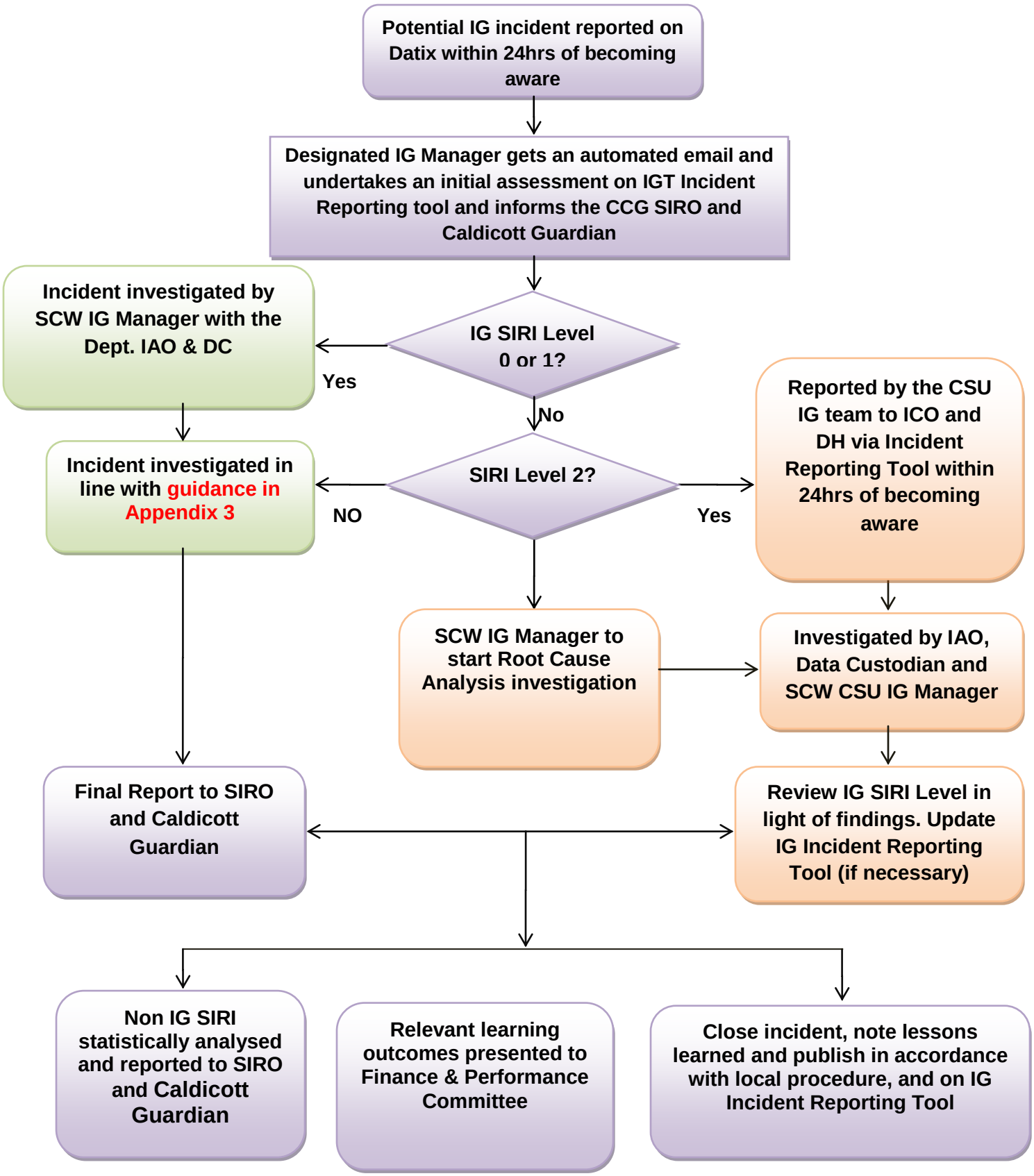
How should you report an incident?

If you discover something that could be considered as an incident you should report it to your department's Data Custodian or line manager and they should ensure that the incident is reported on Datix.

What happens next?

Your department's Data Custodian or line manager or a member of the SCW CSU Information Governance team will investigate the incident and may wish to speak to you directly as things progress.

Appendix 2: Incident Management and Reporting Flowchart



Appendix 3: Assessing the Severity of an Incident and the Categorisation Process

The NHS Digital IG Incident Reporting Tool works on the following basis when calculating the severity of an incident:

There are 2 factors which influence the severity of an IG SIRI – Scale & Sensitivity.

Scale Factors

Whilst any IG SIRI is a potentially a very serious matter, the number of individuals that might potentially suffer distress, harm or other detriment is clearly an important factor. The scale (noted under step 1 below) provides the base categorisation level of an incident, which will be modified by a range of sensitivity factors.

Sensitivity Factors

Sensitivity in this context may cover a wide range of different considerations and each incident may have a range of characteristics, some of which may raise the categorisation of an incident and some of which may lower it. The same incident may have characteristics that do both, potentially cancelling each other out.
For the purpose of IG SIRIs sensitivity factors may be:

i. Low – reduces the base categorisation
iii. High – increases the base categorisation

Categorising Incidents

IG incident categorisation is determined by the context, scale and sensitivity. Every incident can be categorised as level:

1. Level 0 or 1 confirmed IG SIRI but no need to report to ICO, DH and other central bodies/regulators.

2. Level 2 confirmed IG SIRI that must be reported to ICO, DH and other central bodies/regulators.

A further category of IG SIRI is also possible and should be used in incident closure where it is determined that it was a near miss or the incident is found to have been mistakenly reported:

0. Near miss/non-event

Where an IG SIRI has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a “near

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

Baseline Scale	
0	Information about less than 11 individuals
1	Information about 11-50 individuals
1	Information about 51-100 individuals
2	Information about 101-300 individuals
2	Information about 301 – 500 individuals
2	Information about 501 – 1,000 individuals
3	Information about 1,001 – 5,000 individuals
3	Information about 5,001 – 10,000 individuals
3	Information about 10,001 – 100,000 individuals
3	Information about 100,001 + individuals

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Sensitivity Factors (SF) modify baseline scale

Low:	**For each of the following factors reduce the baseline score by 1**
-1 for each	(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
	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
	C) Information unlikely to identify individual(s)
High:	**For each of the following factors increase the baseline score by 1**

+1 for each	(D) Detailed information at risk e.g. clinical/care case notes, social care notes
	(E) High risk confidential information
	(F) One or more previous incidents of a similar type in past 12 months
	(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information
	(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
	(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment
	(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident

Section 3: Where adjusted scale indicates that the incident is level 2, the incident will be reported to the ICO and DH automatically via the IG Incident Reporting Tool.

Final Score	**Level of SIRI**
1 or less	Level 1 IG SIRI (Not Reportable)
2 or more	Level 2 IG SIRI (Reportable)

Example Incident Classification

Examples	
A	Member of staff has access to digital health records as per her job role. Her daughter has recently started dating an older man and the member of staff accessed this man's records and those of other members of his family (5 in total). The main record included reference to a recent STD. Baseline scale factor Sensitivity Factors 0 +1 Detailed information at risk e.g. clinical/care case notes , social care +1 High risk confidential information +1 Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information +1 Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment Final scale point 4 so this is a level 2 reportable SIRI
B	A ward handover sheet containing sensitive personal details of 15 patients from a mental health inpatient ward was found by a member of the public and handed back into the Trust. The gentleman who found the handover sheet said that he found it on the road outside his house. The sheet contained the patient's full name, hospital number and a brief description of their current condition. Baseline scale factor Sensitivity Factors 1 +1 High risk confidential information +1 Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information Final scale point 3 so this is a level 2 reportable SIRI
C	A member of staff reports that the complete paper health records of two of his patients have been inadvertently disposed of. He was working on the records at home when the envelope they were in was thrown into the recycling bin by accident. The bin has been emptied. The clinician works for the Child and Adolescent Mental Health Service. Baseline scale factor Sensitivity Factors 0 +1 Detailed information at risk e.g. clinical/care case notes , social care +1 High risk confidential information +1 Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information Final scale point 3 so this is a level 2 SIRI and reportable

D	A member of staff reports that they have been robbed and their unencrypted laptop has been taken from them. The laptop contained letters to about 25 patients as well as mental health care plans for another 10 patients. The clinician's paper diary was also taken. It contains notes about numerous patients, but not their names. The laptop case also contained their smartcard, ID badge and remote access token. Baseline scale factor Sensitivity Factors 1 +1 Detailed information at risk e.g. clinical/care case notes , social care +1 Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information +1 High risk confidential information Final scale point 4 so this is a level 2 reportable SIRI
E	A Social Services Adult Safeguarding Team send a letter to a Service User's Daughter inviting her to attend a Safeguarding Conference for affected families but sent it to the wrong address. It should have been sent to Mrs J Smith of 22 Nowhere Street but instead was sent to Mrs J Smith of 22 Everywhere Street, an address 5 miles away from where it should have been sent. Baseline scale factor Sensitivity Factors 0 +1 High risk confidential information +1 Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information Final scale point 2 so this is a level 2 reportable SIRI