NHS
North East Hampshire and Farnham
Clinical Commissioning Group

Information Incident Management and Reporting Procedures

Version	2.0
Author	Beverly Carter Head of Information Governance NHS South, Central and West CSU
Date Issued	22 January 2014
Last Review Date	September 2015
Next Review Date	September 2017
Responsibility for Review	NHS South, Central and West CSU

Subject	Information Incident Management and Reporting Procedures
Operative Date	22 January 2014
Author	Beverly Carter, NHS South, Central and West CSU
Review Date	September 2017
For the attention of	All CCG staff
Procedure Statement	This procedure describes the responsibilities for CCG in the management and reporting of Information Incidents
Responsibility for dissemination to new staff	CCG
Training Implications	All staff need to make themselves aware of the procedure content and location for future reference
Further details and additional copies available from:	CCG Governance Manager and CCG Intranet
Approved by	Audit & Risk Committee
Date approved	30 September 2015

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

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	To be confirmed
Website	Location in FOI Publication Scheme	To be confirmed
Keywords:	Incident, Information Governance, Incident Reporting, SIRI	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1			Amendments throughout document to include the new (Feb 15) HSCIC Guidance and Reporting Process	08/09/15
2			References to South CSU amended throughout document to South, Central & West CSU	08/09/15
3		Appendix 4	Inclusion of Assessing the severity of a Cyber SIRI guidnace	08/09/15
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
1	12/11/13	IG Team, South CSU		New document review

2	08/09/15	Jackie Thomas, SCWCSU IG Manager		New HSCIC Guidance & Reporting Process Feb 2015

Contents

1. Summary

1.1 North East Hampshire and Farnham Clinical Commissioning Group recognises the importance of reporting all incidents as an integral part of its risk identification and risk management strategy. The CCG are 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.

1.2 Research has shown that the more incidents are reported and lessons are learned, the less likelihood of further breaches occurring. 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

1.3 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.

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

1.5 The NHS recognises the importance of learning lessons from incidents. Through the introduction of standardised reporting and management arrangements the NHS requires that where incidents occur in one organisation the lessons learnt are shared across all NHS organisations, key stakeholders and individuals accessing care services.

2. Introduction

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

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

2.3 North East Hampshire and Farnham CCG are committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, permanent and temporary staff. The CCGs incident management and reporting procedures are designed to achieve the following objectives:

• a standardised approach to incident management across the CCGs;

• to ensure that learning from incidents is an integral part of the organisations' 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'.

3. Aims and Objectives

3.1 North East Hampshire and Farnham CCG will investigate and manage information incidents including Serious Incident Requiring Investigations (SIRIs) and provide staff with guidelines on identifying and reporting information incidents including near-misses.

3.2 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 CCG policies, fraud or gross misconduct. This document should be read in conjunction with other CCG related policies. Please see item 12 for related CCG policy.

3.3 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.

.

4. Definition of Terms Used

4.1 Incident

4.1.1 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.

4.2 Serious Incident Requiring Investigations (SIRIs)

4.2.1 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 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.

4.3 Adverse Event

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

4.4 A Near Miss

4.4.1 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.

4.5 IG Cyber SIRI

4.5.1 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 organization for example, denial of service attacks, phishing emails and cyber bullying.

5. Roles and Responsibilities

5.1 Accountable Officer for North East Hampshire and Farnham CCG

5.1.1 The role of Accountable Officer for North East Hampshire and Farnham CCG has been assigned to the Chief Officer. Accountable Officers have overall responsibilities for the management of information governance and ensuring appropriate mechanisms are in place to support service delivery and continuity in their organisations.

5.2 Senior Information Risk Owner (SIRO) for North East Hampshire and Farnham CCG

5.2.1 The role of Senior Information Risk Owner (SIRO) has been assigned to the Chief Finance Officer. The SIRO takes ownership of the CCG information risks policy and act as advocate for information risk to the CCG Audit Committees and Governing Bodies by providing written advice on the content of the Statement of Internal Control.

5.3 Caldicott Guardian for North East Hampshire and Farnham CCG

5.3.1 The CCG Caldicott Guardian has been assigned to the Clinical Lead/Chair with responsibilities for reflecting patients' interests regarding the use of Personal Confidential Data (PCD). The Caldicott Guardian will ensure that they are aware of all incidents including unauthorised disclosure of confidential information and promptly reported to the Senior Information Risk Owner (SIRO) for consideration of any necessary actions.

5.4 NHS South, Central and West Commissioning Support Unit Information Governance Service Lead

5.4.1 The Head of Information Governance for NHS South, Central and West Commissioning Support Unit has been appointed to act as the overall Information Governance lead for the CCG and under the approved arrangements, IG service will be provided by the

Information Governance Team of NHS South, Central and West Commissioning Support Unit (CSU) by way of a service specification.

5.4.2 The CSU Head of Information Governance is responsible for ensuring all tasks delegated to NHS South, Central and West Commissioning Support Unit IG Team meets the required standards in line with the service level agreement.

5.5 Information Asset Owner and Data Custodians

5.5.1 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.

5.5.2 Data Custodians should ensure that:

- All IG incidents are reported through the CCG Risk Management Process within 24 hours of becoming aware. SIRI's that occur after normal working hours on a Friday should be
- reported within 24 hours on the next working day. A decision to advise 'on call' communications may be taken.
- 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 Serious Incidents Requiring Investigation';
- recognise actual or potential incidents and take steps to mitigate the risks;
- staff in their departments follow CCG procedures and guidance.

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

6. Reporting, Managing and Investigating Information Incidents

6.1 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* (February 2015 *This guidance supersedes Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation June 2013).*

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

- to identify whether any deficiencies in the application of CCG policies or procedures and/or CCG 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 CSU's Head of IG/IG team will liaise with the directorate/department's IAO, Data Custodian and the CCG's SIRO to ensure incidents are correctly graded and reviewed.
- the CSU's Head of IG, IG team and responsible IAOs and Data Custodians will ensure 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.
- the decision to notify a data subject 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).

6.3 Assessing the severity of an incident

6.3.1 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;

6.3.2 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

6.3.3 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.

6.4 Categorising Information Governance incidents including SIRIs

6.4.1 The categorisation of IG incidents including SIRI 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.

6.5 IG SIRI categorisation review

6.5.1 Incidents which have been categorised as potential level 2 or more will be investigated and considered in greater detail by the CCG SIRO and Caldicott Guardian, the CSU Head of IG and IG Manager. All findings will be reported to the Audit & Risk Committee.

6.5.2 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.

6.5.3 The decision to report a level 2 incident is the responsibility of the SIRO together with the Caldicott Guardian. Once agreed the 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 CSU IG team within 24 hours of becoming aware of the incident and within 24 hours on the next working day if reported on a Friday.

6.6 Reporting to third parties

6.6.1 Where it is suspected that an IG SIRI has taken place, staff should ensure that the SIRO, Caldicott Guardian, directors including 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'.

6.7 Internal Reporting

6.7.1 Any information incident that takes place that is not recorded as a SIRI will be included in SIRO/Caldicott Guardian Issues Log. These are primarily for awareness and to identify trends in minor incidents.

6.7.2 Level 2 IG incidents reports, if agreed by the SIRO, will be presented to the Audit & Risk Committee through the IG Update in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

7. Freedom of Information Requests (FoI)

7.1 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.

7.2 Non-confidential incidents on the CCG and their services will be available to the public through a variety of means including Governing Board 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

8. Action Plans and Audit

8.1 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;

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

9. Record keeping

9.1 A record of all decisions, actions, and recommendations should be kept throughout the investigation and final report. The CCG IAO, Data Custodians, 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;
- files notes with dates are kept of all discussions ;minutes of all meetings are produced.

10. Procedure Review

10.1 In line with the organisations' 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.

11. Training

11.1 North East Hampshire and Farnham CCG recognise the importance of an effective training structure and programme to deliver compliant awareness of confidentiality and data protection and its integration into the day-to-day work and procedures.

11.2 All permanent/contract staff will complete the online mandatory training modules https://www.igte learning.connectingforhealth.nhs.uk/igte/index.cfm within first week of employment, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles.

12. Dissemination and implementation

12.1 This document will be publicised on the website/intranet. Senior managers are required to ensure that their staff understands its application to their practice.

12.2 Awareness of any new content/change in process will be through the staff bulletin in the first instance; 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.

13. Related documents policies and procedures

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

- Information Governance Policy
- Data Subject Access Request Policy
- Records Management Policy
- Information Security
- Confidentiality Policy

14. Equality, diversity and mental capacity

14.1 North East Hampshire and Farnham CCG recognise 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.

14.2 This document was assessed against the NHS South 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.

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

Appendix 1: Staff Guideline on Identifying and Reporting Information Incident

These guidelines apply to all staff including permanent, temporary and contract staff. All incidents must be reported to your line manager, IAO, SIRO, Caldicott Guardian, Data Custodians or the NHS South CSU Information Governance team within 24 hours of becoming aware of the incident. Incidents that occur after normal working hours on a Friday should be reported within 24 hours on the next working day. A decision to advise 'on call' communications may be taken.

What should you report**?**

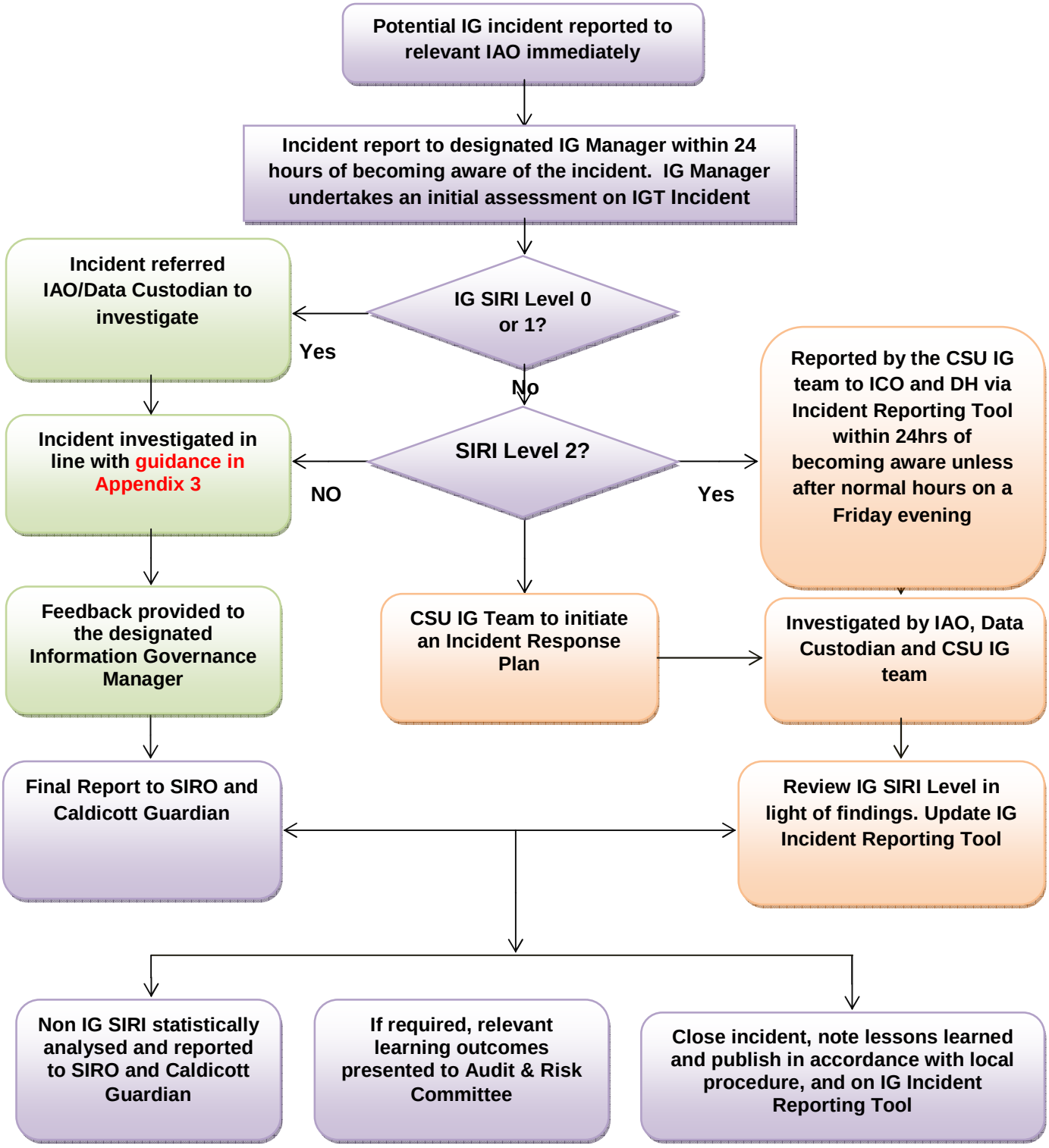
Here are some examples of information incidents that should be reported:

- Finding a computer printout containing Personal Confidential Data (PCD) left unattended;
- Identifying that a fax had been sent to an incorrect recipient outside of the organisation containing either commercially sensitive or personal information.
- finding confidential waste in a 'normal' waste bin;
- losing a mobile computing device with personal information on;
- allowing an individual to access data they have no legitimate reason to view – this could be verbally, paper records or electronic;
- using another member of staff's login/password to access data;
- 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 are not working correctly – potentially because you may have a virus;
- sending a sensitive email or an email containing PCD to unintended recipient or 'all staff' by mistake;
- finding a colleague's password written down on a 'post-it' note;
- A theft or 'break in' has occurred in your place of work;

What happens next?

Your manager, CCG SIRO/IAO/Caldicott Guardian and/or a member of the NHS South 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 IG Incident and the Categorisation Process

The Health and Social Care Information Centre (HSCIC) 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
ii. 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. Confirmed IG SIRI but no need to report to ICO, DH and other central bodies.

2. Confirmed IG SIRI that must be reported to ICO, DH and other central bodies.

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 miss” to enable lessons learned activities to take place and appropriate recording of the event.

<u>The following process should be followed to categorise an IG SIRI</u>

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
	(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

+1 for each	
	(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
	() 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 scoring using the sensitivity factors (IG SIRI)

1	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 – 0 Sensitivity Factors - + 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 organisation or technical safeguards to protect information + 1 Individuals affected likely to suffer substantial damage or distress, including significant embarrassment or detriment **Final scale point 4 so this is a level 2 reportable SIRI**
2	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 – 1 Sensitivity factors - + 1 High risk confidential information + 1 Failure to implement, enforce or follow appropriate organisation or technical safeguards to protect information **Final scale point 3 so this is a level 2 reportable SIRI**
3	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 clinican works for the Child and Adolescent Mental Health Service. Baseline scale factor – 0 Sensitivity factors - + 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 organisation or technical safeguards to protect information **Final scale point 3 so this is a level 2 SIRI and reportable**
4	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 ans remote access token. Baseline scale factor – 1 Sensitivity factors - + 1 Detailed information at risk e.g. clinical/ care case notes, social care + 1 Failure to implement, enforce or follow appropriate organisation or technical safeguards to protect information + 1 High risk confidential information **Final scale point 4 so this is a level 2 reportable SIRI**

5	A Social Services Adult Safeguarding Team sent 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 the Mrs J Smith of 22 Nowhere Street but instead was sent to Mrs J Smith 22 Everywhere Street, an address 5 miles from where it should have been sent. Baseline scale factor – 0 Sensitivity factors + 1 High risk confidential information +1 Failure to implement, enforce or follow appropriate organisation or technical safeguards to protect information **Final scale point 2 so this is a level 2 reportable SIRI**

Appendix 4: Assessing the severity of a Cyber incident

There are 2 factors which influence the severity of a Cyber SIRI – scale and sensitivity.

Scale factors

Whilst any Cyber SIRI is potentially a very serious matter, the scale is clearly an important factor. The scale provides the base categorization level of an incident, which will be modified by a range of sensitivity factors.

0 - No impact: Attack(s) blocked.

0 – False alarm

1 – Individual, internal group(s), team or department affected.

2 – Multiple departments or entire organisation affected.

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 categorization 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 Cyber SIRIs sensitivity factors may be:

Low – reduces the base of categorisation

High – increases the base of categorisation

Catogorising SIRIs

The Cyber SIRI category is determined by the context, scale and sensitivity. Every incident can be categorized as level:

Level 0 or 1 confirmed Cyber SIRI but no alert to HSCIC & DH

Level 2 confirmed Cyber SIRI alert to HSCIC & DH

The following process should be followed to categorise a Cyber SIRI

Cyber sensitivity factors (SF) modify baseline scale

Low:	For each of the following factors reduce the baseline score by 1
-1	(1) A tertiary system affected which is hosted on infrastructure outside health and social care networks

High:	The following factors increase the baseline score by 1
+1	(2) Repeat incident (previous incident within the last 3 months)
	(3) Critical business system unavailable for over 4 hours
	(4) Likley to attract media interest
	(5) Confidential information release (non-personal)
	(6) Require advice on additional controls to put in place to reduce reoccurrence
	(7) Aware that other organisations have been affected
	(8) Multiple attacks detected and blocked over a period of 1 month

Example incident classification scoring using the Sensitivity Factors (Cyber SIRI)

Examples	
1	A Trusts twitter and Facebook accounts are compromised and posts made by a group with forthright views on healthcare provision. The Trust knows a neighbouring provider has also had issues with their social media accounts. Although it is easy to change the accounts password the trust is unsure how to prevent reoccurrence. Baseline scale factor - 1 Sensitivity factors - +1 Likely to attract media interest +1 Require advice on additional controls to put in place to reduce reoccurrence +1 Aware that other organisations have been affected **Final score point 4 so this is a level 2 and would be reportable.**
2	A disgruntled technician from the IT Department who is due to be downgraded

	as part of a reorganisation deletes vast sections of the Active Directory structure (discovered through audit trails.) The organisations' recovery efforts were prolonged due to issue with back up and rollback issues, with IT 'normality' returning 48 hours post event. The organisation does not have a full EPR and so was able to put contingency plans in place and consequently there was not intense media interest. Baseline scale factor – 2 Sensitivity factors - +1 Critical business system unavailable for over 24 hours **Final scale point 3 so this is a level 2 and would generate an alert.**
3	A service user complains that a member of staff has initially befriended them on social media then made a number of inappropriate approaches. The approaches are rejected which leads to the member of staff harassing and trolling the service user. Upon investigation it is discovered the member of staff has utilised business IT equipment and accessed social media sites in line with organisations social media/ fair usage policy. The member of staff has also disclosed details of where the service users resides and treatment plans. Baseline scale factor – 1 Sensitivity factors - +1 Likely to attract media interest **Final scale point 2 so this is a level 2 and would generate an alert. This incident should also go through the IG SIRI classification due to disclosure of confidential information.**
4	An organisations website was subject to large flux on incoming packets from IP addresses outside the U.K that intended for the site to be unavailable. The Trust's new IPS system detected the attached and took appropriate action so that the site suffered no loss of access. Baseline scale factor – 0 no impact: Attack(s) blocked Sensitivity factors – None **Final scale point 0 so this is a level 0 and this should be locally determined whether this should be logged. N.B when determining reporting, consideration should be given to the intelligence value of incidents(s) in informing Cyber responses and not affect (or lack of) a particular incident(s).**
5	An organisation offers free WIFI for patients and visitors in its building. There is also a business WIFI which is widely used with mobile devices used at the point of care to support clinical pathways. As part of a routine examination of audit logs it's believed that a user of the public WIFI has managed to cross

	over from the public WIFI to the business network. There is also some evidence that certain accounts have has unexpectedly elevated rights applied around the same time frame, though due to lack of system wide logging it's not clear what has been affected and whether the two events are connected. The organisation is unsure how to deal with the situation and switches off both public and business WIFI. Baseline scale factor – 2 Sensitivity factors - +1 Critical business system unavailable for over 4 hours +1 Require advice on additional controls to put in place to reduce reoccurrence. **Final scale point 4 so this is a level 2 and would generate an alert**
6	An organisation utilized a 3rd party to provide a salary sacrifice car scheme. The provider's website features the available cars and the ability to calculate your expected contribution. The website is hosted on an external clou in North America which suffers an denial of service attack making the system unavailable for over half the working day. Baseline factors - -1 Sensitivity factors - -1 A tertiary system affected which is hosted on infrastructure outside health and social care networks. **Final scale point -1 so this is a level 0 and would not generate an alert.**