hscic Health & Social Care Information Centre

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation

Applicable to all organisations processing Health, Public Health and Adult Social Care Personal Data

29th May 2015

Version 5.1

Supported by

Department of Health

Revision History

Version	Date	Summary of Changes
V1.0	01/01/2010	First version published by the Department of Health
V2.0	01/06/2013	Second version published by HSCIC – Supersedes V1.0
V3.0	01/06/2014	Third version published by HSCIC – Supersedes V2.0 Updated to offer further clarification on responsibilities to report IG SIRIs using the IG Toolkit Incident Reporting Tool (as defined in the IG Toolkit V12 requirements) and including reference to Caldicott 2 personal data breach related recommendations accepted by Government. Changes approved by Department of Health IG and Standards Policy - Phil Walker.
V4.0	07/11/2014	Fourth version published by HSCIC – Supersedes V3.0 Updated following review of the Incident Reporting Tool by the Health and Social Care represented IG SIRI Design Group and general users after one year implementation. Most significant changes are regarding the Sensitivity Factors used to assess the severity of an incident (including further interpretive guidance) and clarification on timescales for reporting a Level 2 IG SIRI.
V5.0	27/02/2015	Fifth version published by HSCIC – Supersedes V4.0 Updated to included Cyber SIRI functionality.
V5.1	29/05/2015	Minor consistency changes and added description of new 'auto closure' functionality to section 4.4

Note to Readers:

The development of this guidance and the IG Incident Reporting Tool[i] involves representatives from HSCIC External IG delivery Team, the NHS Healthcare Service Providers, Local Authorities, the Department of Health, the IG Alliance, NHS England and the Information Commissioner's Office Enforcement Department. Work is ongoing with these Stakeholders to continually improve the content and enhance the functionality of the Tool and supporting guidance.

Information Commissioner's Office Statement of Support

"The health sector routinely handles extremely sensitive personal data, and it is essential that such information is looked after appropriately. On the occasions where that has not been achieved, it is important that the relevant authorities are made aware at the earliest opportunity. The National Health Service (NHS) has an established culture of informing the ICO of all data breaches, and we welcome the new incident reporting tool which will mandate that reporting process and make it simpler and more efficient.

The ICO has worked closely with the Health and Social Care Information Centre to support the development of the reporting tool and we anticipate that it will become a useful resource for information governance professionals within the NHS."

An IG SIRI Design Group has been set up to ensure that User representation from across the Health and Adult Social Care sector are consulted regarding any proposed developments. This group also have the opportunity to raise operational issues, voice patient/service user perspectives and suggest improvements. Some key areas the group has worked on are further clarification and improvements to the sensitivity factors as noted in Annex A, enhancements to the functionality of the IG Incident Reporting Tool to improve the user experience and review of supporting guidance.

If Users of the tool or members of the public would like to propose any changes in future we would welcome suggestions and ideas through the change request form available via the IG Toolkit website Home page.

Contents

1 The Scope

It is essential that all Information Governance Serious Incidents Requiring Investigation (IG SIRIs) which occur in Health, Public Health and Adult Social Care services are reported appropriately and handled effectively. Commissioned services should be subject to the same requirements to report data breaches to the commissioner of the service and directly through the arrangements described in this document.

What does this guidance cover?

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 SIRI or Cyber SIRI occurs. Organisations should ensure that any existing policies for dealing with IG SIRIs or Cyber SIRI are updated to reflect these arrangements.

Who does this guidance apply to?

This guidance document and supporting IG Incident Reporting Tool product (hosted on the IG Toolkit website)[1] applies to all Organisations providing or supporting Health, Public Health and Adult Social Care services in England.

What is an IG SIRI?

There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. As a guide the scope of an Information Governance Serious Incident Requiring Investigation (IG SIRI):-

- This type of incident will typically breach one of the principles of the Data Protection Act 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.
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals. See Annex E for further definitions and examples of IG SIRI Breach Types.
- Applies irrespective of the media involved and includes both electronic media and paper records relating to staff and service users.
- When lost data is protected e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported down a different route).

[1] Information Governance Toolkit Website - hosting the IG Incident Reporting Tool.

- When the data is protected but there is a risk of individuals being identified then this remains an incident and should be reported. The sensitivity factors within the IG Incident Reporting Tool will reflect that the risk is low.

What is an IG Cyber SIRI?

There are many possible definitions of what a Cyber incident is, for the purposes of reporting a Cyber incident is defined as:-

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 businesses, infrastructure and services."
Source: UK Cyber Security Strategy, 2011

It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation.

These types of incidents could include:

- Denial of Service attacks
- Phishing emails
- Social Media Disclosures
- Web site defacement
- Malicious Internal damage
- Spoof website
- Cyber Bullying
- See Annex H & I For examples and definitions

What should Local Authorities report?

As a point of clarification, for Local Authorities whilst we would recommend that all IG and Cyber SIRI are reported through this tool, a key consideration is where Health related data has been compromised and/or Care services may be impacted. In this case such incidents should be reported using the HSCIC IG / Cyber SIRI process as described in this guide. It is therefore recommended that local procedures are reviewed to incorporate the use of the IG Toolkit Incident Reporting Tool, when appropriate.

Definitions

Where this document refers to incident or SIRI it will generally be applicable to both IG and Cyber SIRI unless explicitly referenced as either.

Where this document refers to an IG SIRI related this is the original data breach / loss event where Level 2 classified reports are alerted to the DH, HSCIC, NHS England and the ICO.

Where this document refers to Cyber SIRI or Cyber incident with or without descriptive "pure" this is the newer cyber reporting where Level 2 classified reports are alerted to the DH and HSCIC only.

What is Personal Data?

As per the Data Protection Act 1998.[2]:

Personal data are data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

What is Sensitive Personal Data?

Sensitive personal data is a subset of Personal Data. Sensitive personal data are personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject,

(b) their political opinions,

(c) their religious beliefs or other beliefs of a similar nature,

(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) their physical or mental health or condition,

(f) their sexual life,

(g) the commission or alleged commission of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

[2] http://ico.org.uk/for_organisations/data_protection/the_guide

What is Confidential Personal Data?

This is personal and usually sensitive personal data that is held subject to an obligation of confidentiality. Clinical data relating to an identifiable individual is almost always confidential and some data recorded by social care staff may also be subject to this obligation.

2 The Requirement

Reporting on the IG Toolkit Incident Reporting Tool:-

All Organisations processing Health, Public Health and Adult Social Care personal data are required[3] to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs[4] to the DH, ICO and other regulators. This has been a requirement since 1st June 2013.

For Cyber SIRI

All Organisations processing Health, Public Health and Adult Social Care personal data are expected to use the IG Toolkit Cyber SIRI extended functionality to contribute to health and social response to the UK's Cyber Security Strategy. Level 2 Cyber Incidents will be notified to the Department of Health and HSCIC only.

Reporting Timescales for incidents:-

The expectation is for Level 2 serious incidents to be reported as soon as possible (usually within 24 hours of a breach being notified/identified locally) and with as much information as can be ascertained at the time. It is understood that further information will become available once the organisation conducts an investigation and the IG Incident Reporting Tool should be kept up to date with regards to any developments or further detail about the incident. A full record of the incident should be complete within 5 working days from when the incident was initially reported.

The reporting of Cyber SIRI Incidents within the tool does not replace local and national service desk reporting. Reported Cyber Incidents will not trigger an operational response.

Local Systems (IG SIRI):-

Local clinical and corporate incident management and reporting tools (including Strategic Executive Information System - STEIS)[5] can continue to be used for local purposes but notifications of IG SIRIs for the attention of DH, NHS England and the ICO must be communicated using the IG Incident Reporting Tool.

3 Level 2 IG SIRIs are sufficiently high profile cases or deemed a breach of the Data Protection Act or Common Law Duty of Confidentiality, and hence reportable to the Department of Health and Information Commissioner's Office. See **Annex A** for further detail on severity levels.

4 Level 2 IG SIRIs are sufficiently high profile cases or deemed a breach of the Data Protection Act or Common Law Duty of Confidentiality, and hence reportable to the Department of Health and Information Commissioner's Office. See **Annex A** for further detail on severity levels.

5 http://www.england.nhs.uk/ourwork/patientsafety/

Closure of report:-

Organisations should ensure that the incident report has been accurately completed and closed in a timely manner after all local incident management and investigation procedures have been followed. See *Important Disclaimer below regarding the publication of closed incidents.

Note that the release of IG Toolkit v.13 will introduce an 'auto closure' feature whereby the auto closure feature will automatically close incidents where no updates to an 'open' record have been undertaken within the last 90 days. Relevant incident reporting users will be notified by email 10 days in advance of planned auto closure and within 24 hours after closure. Further details are described in Appendix A of the 'Incident Reporting Tool User Guide'.

***IMPORTANT DISCLAIMER**

- The Department of Health and the Information Commissioner's Office will automatically receive notifications of **ALL Level 2 IG SIRIs** which have been recorded and saved on this tool. Therefore, all notified level 2 IG SIRIs in particular should be kept up to date so that DH and ICO have view of progress from the initial opening of the incident to closure. See "Checklist Guidance for Reporting, Managing and Investigating IG and Cyber SIRIs" and "The Incident Reporting Tool User Guide" for further detail.
- Ensure that the incident is closed as soon as practicable or appropriate. We would not expect the incident to be in 'Open' status for more than 90 days and the new 'autoclosure' feature will automatically close the incident after 90 days although users will receive a notification email after 80 days (see Appendix A in the Incident Reporting Tool User Guide for more detail on this feature).
- All information recorded under a **"Closed" IG SIRI** record on the Incident Reporting Tool will be published quarterly by the Health and Social Care Information Centre (HSCIC). Organisations must therefore check the content recorded within the IG Incident report before closing the record to ensure that you do not include any information that you would not normally provide or publish yourself if requested under the Freedom of Information Act 2000. Ensure the record is up to date, factual and accurate in content e.g. check spelling, grammar, no person identifiable data etc. Content should be appropriate for publication.
- Cyber information and SIRIs marked as 'Level 2 TBC', "Open", "Withdrawn" or "Duplicate" will not be published by the HSCIC.
- See the "Publication Statement" on the Incident Reporting Tool landing page and accessible via the IG Toolkit Knowledgebase or Publications sections for further detail on our routine publications, what information we share, with whom and for what purpose.
- Only the Department of Health and HSCIC will receive notifications of **ALL Level 2 Cyber SIRIs. If** the Cyber incident is also classed as a Level 2 IG SIRI the ICO will be notified of the IG SIRI information but not the Cyber information entered.

3 The Purpose

The purpose of this guidance is to support Health, Public Health and Adult Social Care service commissioners, providers, suppliers and staff in ensuring that:-

- the management of SIRIs conforms to the processes and procedures set out for managing all Serious Incidents Requiring Investigation;
- there is a consistent approach to evaluating IG SIRIs and Cyber SIRIs;
- early reports of SIRIs are sufficient to decide appropriate escalation, notification and communication to interested parties;
- appropriate action is taken to prevent damage to patients, staff and the reputation of Healthcare, Public Health or Adult Social Care;
- all aspects of an SIRI are fully explored and 'lessons learned' are identified and communicated; and
- appropriate corrective action is taken to prevent recurrence in line with the open data transparency strategy[6].
- Caldicott 2 recommendations (accepted by the Government)[7] are addressed.
- Transparent reporting of incidents
- Contractual obligations are adhered to with regards to managing, investigating and reporting SIRIs in a standardised and consistent manner, including reporting to Commissioners.

Understanding the nature and volume of incidents is the first step towards improving systems and processes to prevent reoccurrence. The monetary penalties served to date can be found on the ICO website and in many cases the organisation concerned was found to have failed in its duty to implement effective organisational and technical security measures to protect personal information in line with the 7th DPA principle or personal information was disclosed in error. This clearly demonstrates that there is an ongoing problem which needs to be addressed.

The Incident Reporting Tool will play a key role in providing visibility and intelligence about incidents. We hope that it will encourage collaborative partnership working amongst key stakeholders to find solutions for addressing issues within the Health and Care sector. It will also go some way to addressing the issues covered by the Information: To share or not to share? Government response to Caldicott Review with regards to personal data breaches.

Cyber SIRI will lead to improved strategic knowledge and understanding of potential future Cyber risks that the increasingly internet connected, multi-delivery partner, multi-networks and divergent assurance regimes health and care sector may encounter.

The consolidated intelligence will be feed back to the network of Senior Information Risk Owners (SIRO's).

3.1 Duty of Care and statutory obligations

Organisations must put in place adequate technical and organisational safeguards, to prevent incidents and have a common law, 'duty of care' and statutory obligation to protect confidential

[6] http://informationstrategy.dh.gov.uk/

[7] https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response

information against such events. Technical safeguards can be thought of as physical protection ranging from ICT passwords and firewalls to building security, whilst organisational safeguards are aimed at employees such as ensuring adequate training, policies and procedures are in place.

An Incident can be caused by a number of factors such as:

- Negligence or human error.
- Unauthorised or inappropriate access, including processing confidential personal data without a legal basis.
- Loss or theft of information or equipment on which information is stored.
- Systems or equipment failure.
- Accidents.
- Unforeseen circumstances such as fire, flood and other environmental factors
- Inappropriate access, viewing information for purposes other than specified/authorised e.g. an individual browsing record about an ex-partner to find their current address.
- Unauthorised access, using other people's user IDs and passwords.
- Poor physical security.
- Inappropriate access controls allowing unauthorised use.
- Lack of training and awareness.
- Hacking attacks.
- 'Blagging' offences where information is obtained by deception.

3.2 Possible Consequences of an IG Incident including Cyber

The negative impact of an IG incident can vary, for instance it may lead to:

- Embarrassment, damage and harm or distress for individuals.
- Loss or denial of service - this could be a physical service e.g. part of the business, or access to certain information necessary for the organisation to function.
- Possible damage to the integrity of information assets
- Litigation.
- Fraud and financial loss.
- Monetary Penalties of up to £500,000 by the Information Commissioners Office.
- Criminal liability.
- Reputational damage.

4. The Checklist

The checklist guidance should be embedded within local processes and procedures which in turn are used by all staff involved in managing SIRIs. It is important to note that much of this checklist will be applicable to 'near misses'. Staff should be encouraged to report IG SIRI "near misses" and the opportunity taken to identify and disseminate the 'lessons learnt'.

Some organisations have found the incident management guidance published by the ICO useful. This guidance can be used to add value to local policies and procedures but cannot be used in place of this HSCIC guidance document which is more focused on the Health, Public Health and Adult Social Care services.

See ICO Guidance on Data Security Breach Management.

All staff should know to whom they should report and escalate suspected or actual SIRIs.

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

Some organisations will have incident management systems already in place which are not solely concerned with information governance or Cyber Security incidents/events. An organisation-wide reporting/management system(s) which covers staff and service user safety, clinical 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.

For hosted teams/departments with access to the IG Incident Reporting Tool it is imperative that local organisation policy and procedures for incident reporting are followed and if an IG SIRI level 2 incident (relating to Health, Public Health or Adult Social Care personal data) occurs the Data Protection Officer and Senior Information Risk Owner (or equivalent) must be informed before notification via the IG Toolkit to the ICO is submitted (Note Cyber SIRI will not be reported to the ICO). In instances where the Host organisation has access to report IG SIRIs via the IG Incident Reporting Tool, they should submit the incident on behalf of the hosted team/department. Where the Host is not registered with the IG Toolkit, the hosted team/department should report this incident themselves through their IG Toolkit access subject to informing the Host organisation Data Protection Officer or as per local procedure.

Where applicable, under terms of agreement there should be a requirement to notify service commissioners in writing of all serious incidents that affect or are likely to affect their contractual obligations. Whilst the commissioner will necessarily be concerned with clinical incidents, information governance incidents should not be overlooked as they can also have a serious effect on patient care. Other NHS contractors should also consider whether it is appropriate to inform service commissioners or other external organisations of IG Serious Incidents Requiring Investigation (IG SIRI), for example if this is likely to lead to a patient complaint/distress/harm.

Where Organisations are expected to report IG SIRIs via the HSCIC IG Incident Reporting Tool hosted on the secure IG Toolkit website they should have regard to this checklist guidance and refer to the

IG Incident Reporting Tool User Guide for further detail on how to access the tool and its functionality etc. For example it is important to note that Level 2 IG SIRIs reported via the tool (excluding Cyber SIRI's) will be automatically relayed on to the ICO and other regulators, as appropriate, when the user chooses to notify. The suggested timescales for recording data breach incidents are detailed below.

The next section deals with management of the incident. The main parts of the process are:

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

This process must be followed by Health, Public Health and Adult Social Care service organisations when reporting a data breach incident.

4.1 Initial Reporting

4.1.1 Suspected incidents

Initial information is often sparse and it may be uncertain whether a SIRI has actually taken place. Suspected incidents and 'near misses' can still be recorded on the IG Toolkit Incident Reporting Tool, as lessons can often be learnt from them and they can be closed or withdrawn when the full facts are known.

4.1.2 Early notification

Where it is suspected that an IG SIRI has taken place, it is good practice to informally notify key staff (Chief Executive, SIRO, Caldicott Guardian, other Directors etc.) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'. For cyber incidents notify the person responsible for any operational response (typically the Head of IT).

Each organisation needs to determine its own notification priorities and have robust policies in place to ensure that appropriate senior staff are notified immediately of all SIRIs or severity level 2 at least. However, the immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.

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

In the case of person identifiable information provided to a recipient organisation for secondary uses, e.g. a transfer of patient data approved under Section 251 of the NHS Act 2006, robust

arrangements must be in place to ensure that the data provider or sponsoring organisation or statutory body is notified of all information governance incidents.

4.1.3 Reporting incidents and timescales

The severity of the incident will be determined by the scale (numbers of data subjects affected) and sensitivity factors selected. If the outcome in terms of the severity of the incident is IG SIRI level 2 (reportable) an email notification will be sent to the HSCIC External IG Delivery Team, DH, ICO and escalated to other regulators, as appropriate (pure Cyber SIRI notification Department of Health (DH) and HSCIC only). If the outcome is IG SIRI level 0 or 1 no notifications will be sent. For further detail on how the severity of an incident is assessed and calculated within the IG Incident Reporting Tool, see **Annex A**. For cyber please see **Annex F.**

Recording and Reporting Timescales via the IG Incident Reporting Tool

Within 24 hours - It is not always possible to pre-judge the severity of an incident until it has been investigated, however, sometimes the incident may be of national media interest, involve particularly sensitive data, include high volume of personal data or potentially cause significant detriment or distress to individuals and may suggest that the IG Incident has the potential to be very serious.

Using your judgement, these types of incidents (Level 2) should be logged and notified on the IG Incident Reporting Tool as soon as possible once the organisation becomes aware of the data breach (usually within 24 hours). Although it is appreciated that at this stage the record of the incident may not be very detailed but it will give the HSCIC, DH and NHS England an early warning of what may become a very serious incident. For example, they may review the incident and determine the need to brief Ministers and/or take other action at a national level if required. For cyber only incidents the interested parties are HSCIC and DH and reporting an incident will not lead to an operational response.

Within 5 days – The expectation is that the reporting organisation should have a full understanding of the Level 2 SIRI and a more detailed report of the incident recorded on the Incident Reporting Tool within 5 days from when the incident was initially reported through your local reporting procedures.

Incident update and Closure - Incidents need to be regularly reviewed and updated during the course of the investigation. When the local investigation is complete and actions taken then the incident should be closed in a practicable timely manner. Organisations do not have to wait for the ICO to respond to their notification in order to close the incident record, as the ICO processes can take a while to execute. If the ICO do request an investigation or take actions against your organisation then the record can be re-opened to update the proceedings. For cyber only incidents the ICO will not be notified.

However, it should be noted that notifications of incidents via the Incident Reporting Tool is for information only and responsibility for managing, investigating, reporting and closing incidents

remains with the data controller organisation responsible for the personal data concerned. HSCIC only provides a standard severity scale for breaches and mechanism to report to the relevant regulators (Cyber only incidents do not report to any regulator). Please note that HSCIC and regulators will only make contact with the reporting organisation if the incident is extremely serious and warrants further investigation or attention. Alert notifications via the IG Incident Reporting Tool are immediate once the user chooses to notify but will not be viewed by regulators outside of normal working office hours Monday to Friday 9am to 5pm.

The decision to inform other regulators will also be taken, dependent upon the circumstances of the incident, e.g. where this involves risks to the personal safety of patients under the care of the NHS then the NHS England Patient Safety Division may also need to be informed. (Cyber only incident do not report to any regulator).

Further information will become available as the investigation takes place and the IG Incident Reporting Tool record should be regularly updated as appropriate. Any significant updates regarding the breach type, severity details and media awareness will trigger a notification from the system to the HSCIC External IG Delivery Team and, where appropriate, this will be relayed to other regulators. (Cyber only incident do not report to any regulator). This will reduce the burden on the organisation in terms of keeping authorities informed and updated as the investigation progresses and is finally closed.

Although the IG Incident Reporting Tool is quite intuitive and context help is provided by most data entry fields to help users make the appropriate selections, the system is still dependant on the User entering quality information. For example, the free text fields, Summary of the incident, Details of the Incident, Data) should be populated with up to date, accurate, factual, non-person identifiable information (see *Important Disclaimer of this guidance), including:

- Date, time and location of the incident.
- Breach Type (definitions and examples of these can be found in

  Annex E). For cyber Annex G
- Clinical Patient Safety aspect Flag (without including detail of the clinical issues which may include personal or sensitive information) (not applicable for cyber)
- Details of local incident management arrangements.
- Confirmation that appropriate and documented incident management procedures are being followed and that disciplinary action will be invoked, where appropriate, following the investigation.
- Description of what happened.
- Theft, accidental loss, inappropriate disclosure, procedural failure etc.
- The number of patients/service users/staff (individual data subjects) involved. (not applicable for cyber)
- The number of records involved. (not applicable for cyber)
- The format of the records (paper or digital). (not applicable for cyber)

- If digital format, whether encrypted or not. (not applicable for cyber)
- The type of record, breach or data involved and sensitivity. (not applicable for cyber)
- Whether the SIRI is in the public domain.
- Whether the media (press etc.) are involved or there is a potential for media interest.
- Whether the SIRI could damage the reputation of an individual, a work-team, an organisation or the Health, Public Health or Adult Social Care sector.
- Whether there are legal implications to be considered.
- Initial assessment of the severity level of the IG SIRI (see **Annex A** for further detail on how this is calculated). **Cyber Annex F**
- Whether the following have been notified (formally or informally):
    - Data subjects
    - Caldicott Guardian
    - Senior Information Risk Owner
    - Chief Executive
    - Accounting Officer
    - Police, Counter Fraud Branch, etc.

- Immediate action taken, including whether any staff have been suspended pending the results of the investigation.

4.2 Managing the incident

- Identify who is responsible for managing the incident and coordinating separate but related incidents
- Identify who is responsible for the investigation and performance management
- Identify expected outcomes
- Identify stakeholders
- Develop and implement an appropriate communications plan
- Preserve evidence
- Investigate the incident (see below)
- Institute formal documentation – this must incorporate version control and configuration management
- Maintain an audit trail of events and evidence supporting decisions taken during the incident
- Where appropriate the Information Commissioner, Department of Health and other regulators will be informed, via the IG Incident Reporting Tool, of any incidents which reach SIRI severity level 2 (reportable)

- Escalate as appropriate (Host organisations, dependent business partners or Commissioners)
- Informing data subjects (e.g. patients, service users, and staff). Consideration should always be given to informing data subjects when personal data about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this is done.
- Identify and manage consequent risks of the incident (these may be IG-related or involve risks to patient safety, continuity of treatment etc.)
- Institute recovery actions
- Invoke organisation's disciplinary procedure as appropriate and document the reasons where it is decided not to take action where such action may be viewed as relevant by external parties
- Institute appropriate counter-measures to prevent recurrence
- Identify risks and issues that, whilst not 'in scope' of the incident, are appropriate for separate follow-up and action
- Level 2 SIRIS recorded on the IG Incident Reporting Tool must include relevant up to date information, particularly under 'Details of incident' and/or 'Actions taken' throughout the management of the incident (in a timely manner). For the reasons stated within this guidance under *Important Disclaimer.

4.3 Investigating the incident

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

- Appoint investigating officer
- Engage appropriate specialist help (IG, IT, Security, Records Management)
- Where across organisational boundaries coordinate investigations (and incident management)
- Investigate – carry out a Root Cause Analysis as per the template using the Incident Decision Tree, which is referenced within NHS England Serious Incident Framework documentation (NPSA tools are still available from the NHS England website. All templates are downloadable. IDT, RCA and report writing and although they need a small amount of flexibility in order to reflect IG rather than patient safety issues they provide a good structure for investigating and reporting IG incidents).

  http://www.npsa.nhs.uk/nrls/improvingpatientsafety/patient-safety-tools-and-guidance/rootcauseanalysis/rca-investigation-report-tools/
- Organisations should be aware of rules of evidence, interviews, preservation of evidence, suspending staff etc.
- Document investigation and findings

- Ensure that content is reviewed with sources for accuracy
- Identify lessons learnt
- Level 2 SIRIS recorded on the IG Incident Reporting Tool must include relevant up to date information, particularly under 'Details of incident' and/or 'Actions taken' throughout the management of the incident (in a timely manner). For the reasons stated on page 9 of this guidance under *Important Disclaimer.

4.4 Final Reporting, Lessons Learned and Closure of the incident

- Set target timescale for completing investigation and finalising reports.
- Produce final report.
- Report reviewed by appropriate persons or appraisal group.
- Sign-off of report – Investigating Officer and Chief Executive, if serious enough.
- Send to the relevant persons and/or committee.
- Identify who is responsible for disseminating lessons learnt.
- Closure of SIRI – only when all aspects, including any disciplinary action taken against staff, are settled.
- Update the IG Incident Reporting Tool – The record cannot be closed until all the data fields are populated including 'Actions taken' and 'Lessons Learned'.
- HSCIC External IG Delivery Team will be notified by email when an incident is closed and will monitor progress.
- For IG SIRI's the board or equivalent body of each organisation in the Health, Public Health and Adult Social Care system should publish details of all data breaches. This should be in the quality report or as part of the annual end of year report by Accountable Officer or may be a performance/governance report for non-NHS organisations e.g. *the quality report of NHS organisations or as part of an annual report or performance report for non-NHS organisations*. See **Annex D** for examples.
- Reports of IG SIRIs should be published on your organisation's website and can be easily exported from the IG Incident Reporting Tool for publication.

4.5 Reporting of the incident (Cyber SIRI)

As the purpose of collecting Cyber Incidents is to inform future direction, provide SIRO feedback but not to provide operation assistance / inform interested parties the process is different to that for IG SIRI:. The broad principles on reporting apply to both IG & Cyber SIRI Incidents, however for cyber please be aware that:-

- Incidents reported will not trigger an operational response.

- Cyber incidents that have been investigated should be categorised according to their severity and sensitivity (Annex F & G)
- Examples Cyber incidents are described in Annex H
- Breach type are defined in Annex I
- Does and Don'ts of Reporting are describe in Annex J

As the purpose of collecting Cyber Incidents is inform future direction / SIRO's and not provide operation assistance or inform regulators the alerts email (for Level 2 Cyber) is sent to DH and HSCIC only.

There are no current plans to publish the results of pure Cyber Incidents. A Cyber incident that is also a data breach is subject the existing IG SIRI reporting and publishing framework.

5 Further assistance

Any queries regarding this guidance or the IG Incident Reporting Tool should be submitted via the IG Toolkit Contact us service.

Any queries regarding the Information Commissioner's Office investigation processes or referenced guidance should be emailed to casework@ico.org.uk

Annex A - Assessing the Severity of the Incident Guide (IG SIRI)

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

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

Please note: Conversely, when lost data is protected e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported down a different route). When the data is protected but risk of individuals being identified remains an incident and should be reported. The sensitivity factors will reflect that the risk is low.

All IG SIRIs entered onto the IG Toolkit Incident Reporting Tool, confirmed as severity level 2, will trigger an automated notification email to the Department of Health, Health and Social Care Information Centre and the Information Commissioner's Office, in the first instance and to other regulators as appropriate, reducing the burden on the organisation to do so.

The 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

Following stakeholder feedback the Sensitivity factors have been revised and are shown on the following page. 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 SIRIs

The IG SIRI category 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 miss" to enable lessons learned activities to take place and appropriate recording of the event.

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 (existing)	
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 the 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

The Incident Reporting Tool will not allow you to select sensitivity factors which would not be relevant based on initial selections. See below for settings and key for A to J sensitivity factors noted above.

When user selects this:	The following sensitivity factors are excluded:
A	D, E
B	D, E, I, J
C	I,J
D	A, B
E	A, B
F	Nothing excluded
G	Nothing excluded
H	Nothing excluded
I	B, C
J	B, C

Step 3: **Where adjusted scale indicates that the incident is level 2, the incident should be reported to the ICO and DH within the reporting timescales noted in this guidance. There is a 'notify later' option within the IG Incident Reporting Tool which can be used to save the incident for a short period to allow you to seek authorisation from local Senior Management or Data Protection Officer to report to Regulators/Central Bodies, if required.**

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

Annex B - Sensitivity Factor Guide (IG SIRI)

(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
Example: The data involved in the incident does not contain information that includes: • Racial or ethnic origin of data subjects • Political opinions of data subjects • Data subjects religious beliefs or other beliefs of a similar nature. • Details as to whether the data subjects are members of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992. • The physical or mental health or condition of data subjects • Sexual life of data subjects • The commission or alleged commission by a data subject of any offence; or • Any proceedings for any offence committed or alleged to have been committed by a data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Confidential information includes clinical records or any data that would enable someone to learn something confidential about someone that they didn't already know. Data that is neither confidential nor sensitive will be demographic data that isn't readily available in the context e.g. an individual's name in the context of who was present at a hospital on a particular day.

(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
Example: The data involved in the incident is already accessible in the public authorities Publication Scheme or otherwise available on the public authorities website. This could be copies of business meeting minutes, copies of policies and procedures that may contain the name of a senior officer or members of staff responsible for signing off such material where they have an expectation that their names and job titles would be accessible. Example: Non confidential information e.g. information from telephone directory which includes data items to which we do not owe a duty of confidence.

(C) Information unlikely to identify individual(s)
Example: Information is likely to be limited demographic data where the address and/or name of data subjects is not included. For example: lists of postcodes within political wards Examples include soundex codes, weakly pseudonymised personal data, and Hospital ID number.

(D) Detailed information at risk e.g. clinical/care case notes , social care notes
Example: This would include Social Worker case notes, Social Care Records, Information extracted from core Social Care systems, Minutes of Safeguarding Review Meetings, Hospital discharge data details, observations of service users, clinical records etc.

(E) High risk confidential information
Example: This would include information where disclosure has been prohibited by Order of a Court and may also include information which its disclosure/handling is governed by statutory requirements, guidance or industry practice. This may include information processed under the following, but not limited to, publications: Information classed as particularly sensitive information: Sexually Transmitted Disease (STD), rape victims, child safeguarding data which would cause considerable distress and damage if it got into the public domain.

(F) One or more previous incidents of a similar type in the past 12 months
Example: More than one incident where an email containing sensitive or confidential data identifying a living individual, has been sent to the wrong recipient. One or more incidents of Social Workers leaving their case recording books with a User of a service. One or more incident of a fax being sent to the wrong fax number or sensitive prints being left on a printer. Could include multiple incidents of the same type which have occurred within a specific department or unit or organisation. Specify within the incident details in terms of whether it is a reoccurring problem within a team, department or throughout the organisation.

(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information
Example: Data has been transferred onto an unencrypted USB device in breach of organisational policy and subsequently lost. Disclosure of information as a result of not complying with an organisations mobile device guardianship policy e.g. left in the car overnight. Example: GP transferring clinical records on unencrypted CD's. Organisations should have policies in place which reduce the risk of data breaches and to ensure that avoidable risks do not occur or re-occur.

(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
Example: Loss of large volumes of personal identifiable data being shared between a public authority and an outsourced/commissioned provider. Disclosure of information relating to sex offenders or vulnerable adults. Where a complaint has been made to the ICO. They are duty bound to investigate if a data breach has taken place. This type of incident would often receive more attention than would otherwise be the case due to the route by which the breach was raised.

(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment
Example: Substantial damage would be financial loss e.g. the loss of Bank Account details of service users, likely resulting in the actual loss of funds of a data subject. Substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation e.g. loss of entire historical record relating to a previously looked after child. Example: Details of individual in witness protection program or individual asked for their ID to be protected.

(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident
Example: Loss of personal information relating to Vulnerable Adults identifying their location, key safe details, reasons for vulnerability. Disclosure of information relating to Data Subjects located in refuge houses, Disclosure of information relating to location of offenders being rehabilitated in the community. Example: Loss of the sole copy of a clinical or social care record. Information where there is no duplicate or back up in existence, so prejudicing continuity of care.

Annex C - Example Incident Classification scoring using the Sensitivity Factors (IG SIRI)

Examples	
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 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**
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 organisational 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 clinician 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 organisational 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 and 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 organisational 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 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 0 Sensitivity Factors +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**	

Annex D - Publishing details of IG SIRIs in annual reports and Statements of Internal Control (SIC)

Principles

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

a) You must ensure that information provided on personal data related incidents is complete, reliable and accurate.

b) You should review all public statements you have made, particularly in response to requests under the Freedom of Information Act 2000, to ensure that coverage of personal data related incidents in your report is consistent with any assurances given.

c) You should consider whether the exemptions in the Freedom of Information Act 2000 or any other UK information legislation apply to any details of a reported incident **or** whether the incident is unsuitable for inclusion in the report for any other reason (for example, the incident is *sub judice* and therefore cannot be reported publicly pending the outcome of legal proceedings).

d) Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Incident Requiring Investigation unless you have reason to believe that the protections have been broken or were improperly applied.

e) Incidents designated as “pure Cyber” are not required to be included in the annual reports and SIC at this time. However cyber incidents that are also IG SIRIs should be included.

Content to be included in Annual Reports

Incidents classified at a IG SIRI severity level 2 (see **Annex A**) are those that are classed as a personal data breach (as defined in the Data protection Act) or high risk of reputational damage, basically reportable to the Department of Health and the Information Commissioner’s Office. These incidents need to be detailed individually in the annual report in the format provided as Table 1 below. All reported incidents relating to the period in question should be reported, whether they are open or closed incidents.

Table 1

SUMMARY OF SERIOUS INCIDENT REQUIRING INVESTIGATIONS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONER'S OFFICE IN 2012-13

Date of incident (month)	Nature of incident	Nature of data involved	Number of data subjects potentially affected	Notification steps
Jan	Loss of inadequately protected electronic storage device	Name; address; NHS No	1,500	Individuals notified by post
Further action on information risk	The [organisation] will continue to monitor and assess its information risks, in light of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems. The member of staff responsible for this incident has been dismissed.			

Notes to producing Table 1

Nature of the incident

Select one of the breach types

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 More detailed descriptions and examples of breach types can be found in **Annex C** of this document.
Category List i) inadequately protected PC(s), laptop(s) and remote device(s) *(including, for example, PDAs, mobile telephones, Blackberrys)* ii. inadequately protected electronic storage device(s) *(including, for example, USB devices, discs, CD ROM, microfilm)* iii. inadequately protected electronic back-up device(s) *(including, for example, tapes)* iv. paper document(s)
Nature of data involved *A list of data elements (e.g. name, address, NHS number).*
Number of data subjects potentially affected *An estimate should be provided if no precise figure can be given.*
Notification steps Individuals notified by post* / email* / telephone* (**delete as appropriate*) Police* / law enforcement agencies* notified (**delete as appropriate*) Media release
Further action on information risk A summary of any disciplinary action taken as a result of the incidents should also be included.

Incidents classified at lower severity level

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

Incidents rated at severity level 0 need not be reflected in annual reports.

Table 2

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN 2013-14		
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**	

Statement of Internal Control (SIC) Guidance

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

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

Any incidence of an IG Serious Incident Requiring Investigation should be reported in the SIC as a significant control issue. For the avoidance of doubt these are those incidents with a severity level 2.

Annex E - IG SIRI Breach Types Defined

Notes for users: These more detailed definitions and examples should help IG Incident Reporting Users select the most appropriate 'Breach Type' category when completing the IG SIRI record on the online tool. However, it is recognised that many data incidents will involve elements of one or more of the following categories. For the purpose of reporting, the description which best fits the key characteristic of the incident should be selected.

Breach Type	Examples / incidents covered within this definition
Lost in Transit	The loss of data (usually in paper format, but may also include CD's, tapes, DVD's or portable media) whilst in transit from one business area to another location. May include data that is; - Lost by a courier; - Lost in the 'general' post (i.e. does not arrive at its intended destination); - Lost whilst on site but in situ between two separate premises / buildings or departments; - Lost whilst being hand delivered, whether that be by a member of the data controller's staff or a third party acting on their behalf Generally speaking, 'lost in transit' would not include data taken home by a member of staff for the purpose of home working or similar (please see 'lost or stolen hardware' and 'lost or stolen paperwork' for more information).
Lost or stolen hardware	The loss of data contained on fixed or portable hardware. May include; - Lost or stolen laptops; - Hard-drives; - Pen-drives; - Servers; - Cameras; - Mobile phones containing personal data; - Desk-tops / other fixed electronic equipment; - Imaging equipment containing personal data; - Tablets; - Any other portable or fixed devices containing personal data; The loss or theft could take place on or off a data controller's premises. For example the theft of a laptop from an employee's

Breach Type	Examples / incidents covered within this definition
	home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk.
Lost or stolen paperwork	The loss of data held in paper format. Would include any paper work lost or stolen which could be classified as personal data (i.e. is part of a relevant filing system/accessible record). Examples would include; - medical files; - letters; - rotas; - ward handover sheets; - employee records The loss or theft could take place on or off a data controller's premises, so for example the theft of paperwork from an employee's home or car or a loss whilst they were travelling on public transport would be included in this category. Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system).
Disclosed in Error	This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information itself hasn't actually been accessed. Examples include: - Letters / correspondence / files sent to the incorrect individual; - Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s55 aspect of reporting); - Failure to redact personal data from documentation supplied to third parties; - Inclusion of information relating to other data subjects in error; - Emails or faxes sent to the incorrect individual or with the incorrect information attached;

Breach Type	Examples / incidents covered within this definition
	- Failure to blind carbon copy ('bcc') emails; - Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data; - Disclosure of data to a third party contractor / data processor who is not entitled to receive it
Uploaded to website in error	This category is distinct from 'disclosure in error' as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include; - Failures to carry out appropriate redactions; - Uploading the incorrect documentation; - The failure to remove hidden cells or pivot tables when uploading a spread-sheet; - Failure to consider / apply FOIA exemptions to personal data
Non-secure Disposal – hardware	The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include; - Failure to meet the contracting requirements of principle seven when employing a third party processor to carry out the removal / destruction of data; - Failure to securely wipe data ahead of destruction; - Failure to securely destroy hardware to appropriate industry standards; - Re-sale of equipment with personal data still intact / retrievable; - The provision of hardware for recycling with the data still intact
Non-secure Disposal – paperwork	The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include; - Failure to meet the contracting requirements of principle seven when employing a third party processor to remove / destroy / recycle paper; - Failure to use confidential waste destruction facilities (including on site shredding); - Data sent to landfill / recycling intact – (this would include refuse mix up's in which personal data is placed in the general waste);

Breach Type	Examples / incidents covered within this definition
Technical security failing (including hacking)	This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include: - Failure to appropriately secure systems from inappropriate / malicious access; - Failure to build website / access portals to appropriate technical standards; - The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of industry best practice; - Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces); - Failure to implement appropriate controls for remote system access for employees (for example when working from home) In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate this risk. **A technical security incident may also be a Cyber incident (please see Cyber guidance within this document)**
Corruption or inability to recover electronic data	Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care / adverse clinical outcomes. For example; - The corruption of a file which renders the data inaccessible; - The inability to recover a file as its method / format of storage is obsolete; - The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible
Unauthorised access/disclosure	The offence under section 55 of the DPA - wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller. **Example (1)** An employee with admin access to a centralised database of patient details, accesses the records of her daughter's new

Breach Type	Examples / incidents covered within this definition
	boyfriend to ascertain whether he suffers from any serious medical conditions. The employee has no legitimate business need to view the documentation and is not authorised to do so. On learning that the data subject suffers from a GUM related medical condition, the employee than challenges him about his sexual history. **Example (2)** An employee with access to details of patients who have sought treatment following an accident, sells the details to a claims company who then use this information to facilitate lead generation within the personal injury claims market. The employee has no legitimate business need to view the documentation and has committed an offence in both accessing the information and in selling it on. A recent successful prosecution for a s55 offence: http://ico.org.uk/news/latest_news/2013/gp-surgery-manager-prosecuted-for-illegally-accessing-patients-medical-records-02122013
Other	This category is designed to capture the small number of occasions on which a principle seven breach occurs which does not fall into the aforementioned categories. These may include: - Failure to decommission a former premises of the data controller by removing the personal data present; - The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data; - Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets). This category also covers all aspects of the remaining data protection principles as follows: - Fair processing; - Adequacy, relevance and necessity; - Accuracy; - Retaining of records; - Overseas transfers

Annex F - Assessing the Severity of the Incident Guide (Cyber SIRI)

Although the primary factors for assessing the severity level is the criticality and scale of the incident, for example the potential for impact on confidentiality, integrity or availability. If more information becomes available, post incident investigation the Cyber SIRI level should be re-assessed.

Please note: Conversely, when targeted systems are protected e.g. by an Intrusion Prevention System, so that no services are affected. The sensitivity factors will reflect that the risk is low.

All Cyber SIRIs entered onto the IG Toolkit Incident Reporting Tool, confirmed as severity level 2, will trigger an automated notification email to the DH and HSCIC.

The 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 a Cyber SIRI – Scale & Sensitivity.

Scale Factors

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

Cyber Baseline Scale*	
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.

*See context level help

A further category of Cyber 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. No impact: Attack blocked
0. False Alarm

Where a Cyber 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

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 Cyber SIRIs sensitivity factors may be:

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

Categorising SIRIs

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

1. Level 0 or 1 confirmed Cyber SIRI but no alerting to HSCIC & DH.
2. Level 2 confirmed Cyber SIRI alerting to HSCIC & DH.

The following process should be followed to categorise a Cyber SIRI

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

Cyber Sensitivity Factors (SF) modify baseline scale

Low:	For each of the following factor 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 for each	(2) Repeat Incident (previous incident within last 3 months)
	(3) Critical business system unavailable for over 4 hours
	(4) Likely 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

Annex G - Sensitivity Factor Guide for Cyber SIRIs

(1) A tertiary system affected which is hosted on infrastructure outside health and social care networks.
Example: A staff discount site (that does not contain personal details), an externally hosted training website, an external forum site, an outsourced externally hosted estates management system. Does not include any key information assets (irrespective of hosting arrangements).

(2) Repeat Incident (previous incident within last 3 months)
Example: A 2nd denial of service attack occurs at an organisation within 3 months of the 1st.

(3) Critical business systems unavailable for over 4 hours
Examples of critical information systems could include electronic patients record systems, key departmental systems e.g. Theatres Management, file storage, network and telephone infrastructure, Infrastructure services (active directory, dhcp, dns etc.) and critical firewalls. N.B. These can include key information assets but also encompass key infrastructure services.

(4) Likely to attract media interest
Example: Any Cyber incident that leads to compromised systems within the health and social care sectors is likely to be of media interest due to increased focus on all things Cyber.

(5) Confidential information release (non-personal)
Examples: Non-personal confidential information could include unabridged board meeting meetings, corporate financial planning information and planned service transformation information (restricting, closure and merger of services).

(6) Require advice on additional controls to put in place to reduce reoccurrence
Example: Where a Cyber incident has occurred and appropriate control(s) (physical, administrative or technical) may well be available however the organisation may need consultation and resources to action them. Such as patching, a system which is utilised by several organisations.

.

(7) Aware that other organisations have been affected
Example: A shared infrastructure Cyber incident (e.g. a local healthcare economy COIN) , a mass malicious spam which is known to have effected multiple organisations or a social engineering attack with telephone callers impersonating the local IT section in order for users to take compromising actions reported at multiple organisations.

(8) Multiple attacks detected and blocked over a period of 1 month
Example: A significant number of unknown source IP's trying to access a known destination and service blocked by a firewall/IPS. Malicious and repeated spam emails being blocked at an email gateway. The volume of attempts/attacks reporting threshold should be a reflective of the type and nature organisation and there is no desire to report per event.

Annex H - 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 scale 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 organisation's recovery efforts where prolonged due to issues with backup 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 4 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 a member of 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 the 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 the disclosure of confidential information.**

4	An organisations web site is subject was subject to large flux on incoming packets from an IP addresses outside the U.K. that intended for the site to be unavailable. The trust's new IPS system detected the attack 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 the incident(s) in informing Cyber responses and not the affect (or lack of) a particular incident(s).**
5	An organisation offers free WIFI for patients and visitors in its buildings. There is also a business WIFI which is used 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 Wi-Fi to the business network. There is also some evidence that certain accounts have had unexpectedly had elevated rights applied around the same time frame, though due to lack of system wide logging there it's not clear what has been effected 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 utilises 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 cloud in North America which suffers a denial of service attack making the system unavailable for over half the working day. Baseline scale factor -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**

	N.B. If this scenario was for a key information asset the negative sensitivity factor would not be appropriate. If the systems held more personal details potentially including salary and the attack was a hacking one this should be re-evaluated as both as a Cyber and IG SIRI.

Annex I - Breach Types Defined (Cyber SIRI)

Notes for users: These more detailed definitions and examples should help Cyber Incident Reporting Users select the most appropriate 'Cyber Incident Type' category when completing the IG/Cyber SIRI record on the online tool. However, it is recognised that many data incidents will involve elements of one or more of the following categories. For the purpose of reporting, the description which best fits the key characteristic of the incident should be selected. Some of the elements can be quite technically detailed and it is recommended that however provides an IT security service to you is involved in completion,

Cyber Incident Type	Examples / incidents covered within this definition
Hacking	A deliberate attempt to comprise infrastructure or Information assets usually associated with an external (internet facing) attack.
Denial of Service (DOS)	A deliberate attempt to make infrastructure or information assets unavailable to access. Commonly this would be internet attack that floods the target with requests over its capacity to process. This leads to the target system being unavailable.
Phishing emails	Mass emails with malicious intent of attempting receivers to disclose generally sensitive emails. May be combined with spoof website(s).
Social Media Platforms	Any form of disclosure from the organisation staff through social media channels that discloses sensitive information (personal or corporate) or brings that organisation or the wider health and social care sector into disrepute.
Web site defacement	This is a deliberate attempt to alter the contents of an organisations web site(s). The motivation is normally to further a particular cause and / or to embarrass the target organisation.
Malicious internal damage	This category is cover 'malicious insider threats' - Deletion / modification of information assets - Compromising infrastructure deliberately The motivation for the damage could be a disgruntled employee or a third party organisation losing a support contract.
Spoof website	This is a website that purports to be a legitimate site but is however spoofed. These are commonly used to gather personal information from the victims and can form part of spam mail distribution. The spoof website true address hidden in a link. The professional presentation of a spoof website can be virtually indistinguishable to the legitimate original site. Main indicators of its status is the web site address (varies from the original) and the type of personal information it asks for.

Cyber Incident Type	Examples / incidents covered within this definition
Cyber bullying	This is the category covers incidents where member of staff initiates threatening or intermediating behaviour to another member of staff or outside person most commonly through mail or social media channels. It is expected that either the initiator or receiver could be linked back to the organisation (email address or tag etc.).
Other	This category is designed to capture more unusual or emergent type of incident. - A new type of Cyber incident that utilises a new and distinct attack vector. - An incident type that could be classified under a significant number of types with no one type being particularly prevalent.

Annex J - Cyber SIRI Dos and Don'ts

Dos:

Report incidents that have closed and could be of benefit SIRO's and the wider health and social care sectors.

Seek appropriate technical advice during completion or if appropriate to your organisation delegate access to your IT service to log an incident. Contact the helpdesk if you require further assistance.

Where appropriate group same type incidents into one incident record.

Do report up to your level of capability / capacity E.g. If you have a new and sophisticated IPS that can detect / prevent new attack vectors please report if you consider useful even if your IPS blocked it. Conversely if your capabilities are limited report what closed incidents you can.

Please give feedback on the tool to help and inform future development direction

If Users of the tool or members of the public would like to propose any changes in future we would welcome suggestions and ideas through the change request form available via the IG Toolkit website Home page.

Don'ts

Don't report ongoing incidents with an expectation of an operational response.

Don't report every possible log entry on your firewalls, IPS and IDS. We are interested in significant incidents that require investigation.

Don't report general phishing emails that go to private email addresses.

Don't report Cyber incidents that happen outside of work unless there is some linkage to work (e.g. a Cyber incident involving remote home working)

Don't report Social Media Incidents unless there is a direct link to work (e.g. names / organisations inappropriately identified)

[i] The Incident Reporting Tools reference covers both IG SIRI and Cyber Security Incidents