**Serious Incidents Procedure**

**CONTENTS**

[1 Introduction 1](#_Toc449515378)

[2 Scope & Definition 2](#_Toc449515379)

[2.1 Who should report Serious Incidents 2](#_Toc449515380)

[3 Responsibilities 2](#_Toc449515381)

[3.1 All Staff 2](#_Toc449515382)

[3.2 Chief Operating Officer 2](#_Toc449515383)

[3.3 Responsible Director/ Director on Call 3](#_Toc449515384)

[3.4 Lead Managers / Senior Managers / Line Managers 3](#_Toc449515385)

[3.5 Key personnel - IG Incident Management 3](#_Toc449515386)

[4 Definitions 4](#_Toc449515387)

[4.1 Never Events or Near Misses 4](#_Toc449515388)

[4.2 Serious Incidents 4](#_Toc449515389)

[4.3 Cyber Incidents 4](#_Toc449515390)

[4.4 Safeguarding Incidents 5](#_Toc449515391)

[5 Procedure 5](#_Toc449515392)

[5.1 Initial Reporting 5](#_Toc449515393)

[5.2 Managing the Incident 5](#_Toc449515394)

[5.3 Investigating the incident 6](#_Toc449515395)

[5.4 Final Reporting, Lessons Learned and Closure of incident 6](#_Toc449515396)

[5.5 Contacts: 6](#_Toc449515397)

[5.6 APPEDIX C - IG Serious Incident (IG SI) Notification Flow Chart Process 7](#_Toc449515398)

[6 Revision history 8](#_Toc449515399)

# Introduction

### This procedure describes the CCG’s approach to capturing, reporting, managing and investigating information governance serious incidents.

### Sets out steps and actions to be taken in the event of an Information Governance (IG) Serious Incident Requiring Investigation (SIRI) involving personally identifiable data (PID) occurring at Stockport CCG or any of their hosted organisations.

The intention of the CCG is to ensure that all Information Governance related Serious Incidents that occur in the organisations are reported and managed in a consistent and effective manner so as to minimise the risk of harm to individuals and the CCG.

The Procedure outlines the responsibilities of the CCG in relation to performance management of IG and Cyber serious incidents and ensures that:

* Management of these incidents conforms to the processes and procedures for managing SIRI’s
* Provides a consistent approach to evaluating IG and Cyber SIRI’s
* Early reports of SIRI’s provide sufficient information to decide appropriate escalation and communication
* Appropriate action is taken to prevent damage to patients, staff and the reputation of Healthcare, Public Health and Social Care
* All aspects of a SIRI are fully explored and ‘lessons learned’ are identified and communicated
* Appropriate corrective and preventative action is taken to avoid recurrence
* Caldicott 2 recommendations are addressed
* Transparent reporting of incidents
* Contractual obligations are adhered to eg managing investigating and reporting SIRI’s in a standard and consistent manner

### This procedure should be used by all staff and contractors working for, or supplying services for the CCG including independent contractors (such as General Practitioners) insofar as they are using CCG-supplied computer equipment or information.

### This procedure is associated with and is a supplement to the CCG’s [Information Governance Framework](http://nww.intranet.stockportccg.nhs.uk/Policies%20procedures%20%20guidance/IG%20Framework%20and%20Policy.docx) and the [Information Governance & Risk Management Policy.](http://nww.intranet.stockportccg.nhs.uk/Policies%20procedures%20%20guidance/Information%20Governance%20and%20Risk%20Management%20Operational%20Policy.pdf)

### This procedure is live on 25th November 2015.

# Scope & Definition

## Who should report Serious Incidents

### This procedure applies to all IG incidents (including Cyber incidents) and near misses occurring at the CCG site.

### Any IG incidents occurring at Provider sites are expected to be report all serious incidents. Incidents will be reported (including never events, and serious health-care associated infections) directly to the Quality and Provider Management Team. This includes any organisation which is accountable to the CCG through contracting and commissioning arrangements, using the CSU’s Procedure located on the [Peoples Direct website](http://nww.gmcsu-ext.salford.nhs.uk/sites/pd_ccg/Interface/Home.aspx?ReturnUrl=%2fsites%2fpd_ccg%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252Fsites%252Fpd%255Fccg&Source=%2Fsites%2Fpd_ccg).

# Responsibilities

## All Staff

### All staff are responsible for:

* Making themselves aware of the IG Serious Incident reporting procedure
* Reporting adverse incidents if they were involved, have witnessed or discovered
* Being aware of the need to report ‘Near Miss’ or ‘Never Event’ incidents
* Familiarising themselves with organisational procedures and the actions needed in case of adverse incident
* Availing themselves of training opportunities for incident reporting, incident management and other related issues

## Chief Operating Officer

### In the event of an IG Serious Incident (SI) the Chief Operating Officer must be notified who will have overall accountability for the IG SI and ensure that:

* Satisfactory immediate steps have been taken to minimise risks
* Necessary communication channels have been established
* Appoint a Chair for the investigation panel (if applicable)
* Approve the Terms of Reference and membership of the investigation panel (if applicable)

## Responsible Director/ Director on Call

In the event of an IG Untoward Incident (SI), the Lead Director (if out of hours the Director on-call) will ensure that:

* The Chief Operating Officer and Key Personnel are informed of the incident
* Immediate remedial action/s taken by the most senior person on the scene are reviewed
* An IG SI Notification Form has been completed by the Lead Manager and counter-signed
* Appropriate arrangements are made to preserve the evidence
* Hazards are appropriately removed
* Security and safety of all individuals is achieved
* Investigation and implementation of local action plans in relation to IG SIs is undertaken and that this procedure is followed in their management
* Ensure that the recommendations from the investigation reports for serious incidents are implemented and monitored.

## Lead Managers / Senior Managers / Line Managers

It is the responsibility of each Lead Manager / Senior Manager / Line Manager to:

* Check that all details are correct
* Ensure all possible measures are taken to minimise adverse incidents within his/her area
* Investigate all adverse incidents, in accordance with CCG investigation procedure
* Take all necessary action to prevent re-occurrence
* Promote and encourage staff to report all adverse incidents, including ‘Near Misses’
* Ensure IG SI Notification Form is completed and counter-signed by the Lead Director
* Ensure all recommendations are implemented
* Senior Managers are also responsible for presenting the outcome of investigations/ recommendations in their Directorate Team Meetings or equivalent.

## Key personnel - IG Incident Management

### The Chief Finance Officer is the Senior Information Risk Owner (SIRO) for the CCG who will act as the lead for IG Serious Incidents.

### In the absence of the SIRO, the Caldicott Guardian of the CCG or nominated Deputy Caldicott Guardians will fulfil lead officer responsibilities for IG Serious Incidents.

### In the absence of both the SIRO and Caldicott Guardian or nominated Deputy Caldicott Guardians the on-call Director will fulfil lead officer responsibilities.

### The Board Secretary and Head of Governance will be responsible for

### Notifying NHS England (who performance manage all CCG SI’s) within 24 hours of notification of the incident

* Logging the incident on the [IG Toolkit](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423465495179781&uid=75463&cb=a665220d-458e-4805-bfd2-ec90b4d9588b&lnv=12&clnav=YES)
* Monitoring the investigation of all IG SIRI’s
* Ensuring that the Risk Register is updated
* Classification and privacy impact assessment of IG SI issues
* Assurance of compliance with NHS IG SIRI reporting requirements
* Action planning for the resolution of IG SiRI’s
* Managing the corporate response to IG Serious Incidents and reporting Serious Incidents to the Governing Body.

### Lead Directors are responsible for investigation and implementation of local action plans in relation to IG Serious Incidents and ensuring that this procedure is followed in their management.

# Definitions

## Never Events or Near Misses

### Never Events are avoidable occurrences attributed to NHS systems, services or staff which have a serious detrimental consequence to patient’s staff or the general public.

### Nationally, a core list of Never Events and a process for monitoring them has been developed by the [National Patient Safety Agency](http://www.npsa.nhs.uk/).

## How to categorise an IG SIRI

### To assess the severity of an IG incident, the [IG Toolkit site](https://nww.igt.hscic.gov.uk/HomeLoggedIn.aspx?tk=425004675331376&uid=75463&cb=1c571cf0-5e8d-49ff-aec0-eb94ab3c8684&lnv=7&clnav=YES), within the Incident Reporting section and review the ‘Checklist Guidance for Reporting, Managing and Investigating Incidents’ document - Annex A.

### If still unsure, call the HSCIC IG Team 0300 303 5678.

## Serious Incidents

### A serious incident (SI) is an incident that occurred in relation to Health, Public Health and Adult Social Care personal data resulting in one of the following:

1. Where an incident breaches one of the principles of the Data Protection Act and/or the Common Law Duty of Confidentiality
2. Unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people’s privacy
3. Personal data breaches which could lead to identify fraud or have other significant impact on individuals.
4. Applies irrespective of the media involved and includes both electronic media and paper records relation to staff and service users
5. When lost data is protected eg by appropriate encryption, so that no individuals data can be accessed, then there is no data breach
6. 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.

## Cyber Incidents

### A Cyber incident is anything that could (or has) compromised information assets within Cyberspace i.e. internet, information systems that support the CCG and infrastructure service. Types of Cyber incidents include:

### Phishing emails

### Social Media Disclosures

### We site defacement

### Malicious internal damage

### Spoof website

### Cyber Bullying

### For further information on types of Cyber breaches see Annex I [Checklist Guidance for Reporting, Managing and Investigating Incidents](http://nww.intranet.stockportccg.nhs.uk/SitePages/Home.aspx)

### To assess the severity of cyber incidents see Annex H of the [Checklist Guidance for Reporting, Managing and Investigating Incidents](http://nww.intranet.stockportccg.nhs.uk/SitePages/Home.aspx)

### The CCG’s Serious Incidents (SI’s) are likely to involve the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals.

## Safeguarding Incidents

### Some serious incidents will also be safeguarding incidents and it will be necessary to cross reference the actions being taken against the [Safeguarding Policy](http://nww.intranet.stockportccg.nhs.uk/Policies%20procedures%20%20guidance/Safeguarding%20Children%20and%20Vulnerable%20Adults%20Policy.docx). If in doubt, advice can be sought from the safeguarding team.

# Procedure

## Initial Reporting

### IG and Cyber incidents are both referred to as SIRI’s within this procedure unless explicit references are made.

### Notification of IG SIRI’s Serious Incidents Requiring Investigation (SIRI’s) of personal and confidential data breaches must be communicated using [The IG Toolkit Incident Reporting Tool](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423463694709124&uid=75463&cb=609d2d5c-0565-44c5-a238-d71cff6cedd5&lnv=12&clnav=YES).

### The [IG Toolkit Incident Reporting Tool](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423463694709124&uid=75463&cb=609d2d5c-0565-44c5-a238-d71cff6cedd5&lnv=12&clnav=YES).is used to notify the [Department of Health](https://www.gov.uk/government/organisations/department-of-health) (DoH) and the [Information Commissioners Office](https://ico.org.uk/) (ICO) of level 2 Information Governance Serious Incidents Requiring Investigation (SIRI).

### Commissioned Providers should notify the Quality & Provider Management Team at the CCG as detailed in the Shared Services procedure located on the [Peoples Direct website](http://nww.gmcsu-ext.salford.nhs.uk/sites/pd_ccg/Interface/Home.aspx?ReturnUrl=%2fsites%2fpd_ccg%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252Fsites%252Fpd%255Fccg&Source=%2Fsites%2Fpd_ccg) and via the [Strategic Executive Information Systems](https://www.england.nhs.uk/patientsafety/serious-incident/) (STEIS). Commissioned Providers Level 2 SIRI’s should be reported as soon as possible (usually within 24 hours of a breach). A full record of the incident should be completed within 5 working days from when the incident was initially reported.

### An IG related Serious Incident can happen because of a number of reasons:

* Loss or theft of data or equipment on which data is stored.
* Inappropriate access controls allowing unauthorised use.
* Equipment failure Human error.
* Unforeseen circumstances such as a fire or flood
* Hacking attack.
* ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

### For guidance on how to complete the online form, see the [Incident Reporting Tool User Guide](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423463694709124&uid=75463&cb=35697189-f0d2-40e6-9cc5-a847dab7a179&lnv=12&clnav=YES) on the Incident Reporting page of the IG Toolkit.

### For further guidance on types of breaches, what constitutes personal data and sensitive personal data breaches and how they are categorised see the [Checklist Guidance for IG Serious Incidents Requiring Investigation](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423463694709124&uid=75463&cb=35697189-f0d2-40e6-9cc5-a847dab7a179&lnv=12&clnav=YES) on the Incident Reporting page of the IG Toolkit.

### When a IG SIRI level 2 incident occurs, the Data Protection Officer and Senior Information Risk Owner must be informed before notification via the IG Toolkit.

### A IG SIRI should also be recorded on the CCG [Report an Incident](http://hex/safeguardcom/index.aspx?sid=%20) system located on the front page of the CCG SharePoint.

## Managing the Incident

### Identify who is responsible for managing the incident and who is responsible for the investigation.

### Preserve evidence.

### Investigate and document the incident and findings using suitably controlled documentation i.e. dated and version controls.

### Maintain an audit trail of events and evidence.

### Report the incident to the Information Commissioner, Department of Health by recording and updating the incident if severity level is 2 or above.

### Escalate where necessary i.e. business partners.

### Inform data subjects i.e. patients, service user or staff.

### Identify and manage risks.

### Institute recovery actions.

### Invoke disciplinary procedure if appropriate.

### Institute appropriate counter measures to prevent reoccurrence.

## Investigating the incident

### Appoint investigating officer and scope ie across organisational boundaries

### Engage appropriate specialist help ie IG, IT, Security, Records Management etc.,

### Investigate by conducting a root cause analysis following the template reference within [NHS England Serious Incident Framework](https://www.england.nhs.uk/patientsafety/wp-content/uploads/sites/32/2015/04/serious-incidnt-framwrk-upd2.pdf) documentation, which contains downloadable templates.

### Document findings and investigation.

### Identify lessons learnt.

## Final Reporting, Lessons Learned and Closure of incident

### Set timescale for completing investigation and finalising reports.

### Produce final report.

### Report reviewed by appropriate person or group.

### Sign off of report by Investigating Officer and Chief Operating Officer.

### Circulate to relevant persons or committees.

### Identify who is responsible for disseminating lessons learnt.

### Close SIRI, when all actions are settled, including staff disciplinaries.

### Update [The IG Toolkit Incident Reporting Tool](https://nww.igt.hscic.gov.uk/IncidentReportingMenu.aspx?tk=423463694709124&uid=75463&cb=609d2d5c-0565-44c5-a238-d71cff6cedd5&lnv=12&clnav=YES)

### Report to the Governing Body all data breaches as part of the end of year report.

### Report of IG SIRI’s should be published on the CCG’s website.

## Contacts:

For further information or enquiries in relation to any aspect of this document, please contact:

**Senior Information Risk Owner**

(Chief Finance Officer )

Tel: 0161-426 5603

**Caldicott Guardian**

(Clinical Director of Public Health)

Tel: 0161-249 4223

**Head of Information Governance and Board Secretary**

Tel: 0161-426 5210

## 

## APPEDIX C - IG Serious Incident (IG SI) Notification Flow Chart Process

**Lead Manager of Service immediately notifies:**

• Relevant CCG Director /

• On-call Director isoutcorworking

hours

**Within Core Working Hours**

**Outside Core Working Hours**

**On-call PCT Director Notifies:**

* Relevant CCG Director
* Senior Information Risk Owner (SIRO)
* Caldicott Guardian
* Board Secretary & Head of Governance
* Chief Operating Officer

**On call CCG Director/Lead Manager**

* Completes an IG SI Notification (through SharePoint or form) and sends to key personnel

**CCG Director Notifies:**

* Senior Information Risk Owner (SIRO)
* Caldicott Guardian
* Board Secretary & Head of Governance
* Chief Operating Officer

**Lead Manager:**

* Completes IG SI Notification on SharePoint / form and faxes to above Key Personnel
* Initiates an investigation

**Information Governance Lead/SIRO**

* Notifies NHS England verbally within 24 hours of notification of the incident
* Logs the incident on STEIS and/or IG Toolkit (if IG incident) when completed and authorised IG SI Notification Form received

**Information Governance Lead**

* Notifies NHS England verbally within 24 hours of notification of the incident
* Logs the incident on STEIS and/or IG Toolkit (if IG incident) when completed and authorised IG SI Notification Form received

# Revision history

| **Version** | **Date** | **Changes** | **Approved by** |
| --- | --- | --- | --- |
| 4 | 12/5/16 | Added 4.4 How to categorise incidents. | Kathy Taylor |
| 3 | 27/4/16 | Added 4.4 Safeguarding Incidents and hyperlink | Anita Rolf |
| 2 | 10/12/15 | Clarified the logging of IG and Cyber Incidents on the IG Toolkit and cross referenced with relevant sources of guidance and information. References to STEIS clarified. | Kathy Taylor |

*Administrative changes or changes to Legislation will be amended by the Compliance Support Officer. Any significant changes to processes or procedures will be approved by the process owner / Director.*