North, Central and South Manchester
Clinical Commissioning Groups

NHS

Corporate Policy

Incident Reporting and Management Policy (Including Serious Incidents)

Version: **1.1**

Date Approved: **May 2014**

Document Control Sheet

Title of document:	Incident Reporting and Management Policy(including Serious Incidents)		
Supersedes:	PCT Policy		
Placement in Organisation:	Manchester CCGs		
Consultation / Stakeholders	CCG Leads Quality Teams City Wide Commissioning Corporate Services Team		
Author(s) name:	**Kate Lord**, Quality Lead, Shared Performance and Quality Team **Jan Eccleston**, Deputy Head of Quality and Incident Reporting, City Wide Commissioning Team **David Smith**, Corporate Governance Manager, Shared Corporate Services Team		
Department / Team:	City Wide Quality Team City Wide Commissioning Team City Wide Corporate Services Team		
Approved by:	CCG Quality Committees		
Approval date:	May 2014	Review date:	May 2017
Implementation Date:	June 2014		
Implementation Method:	CCG Website Manchester Matters		
This document is to be read in conjunction with the following documents:			

Version Control

Version	Date	Brief description of change
V.1	Jan 14	First Draft of Policy sent to CCG Governance Leads
V.1.1	Jun 14	Equality Analysis added as an Appendix

PLEASE NOTE: the formally approved copy of this document is held on North, Central and South CCG's website. Printed copies or electronic saved copies must be checked to ensure they match the current online version.

Contents

Appendices

1.0 Policy Statement

1.1 This policy underpins the Clinical Commissioning Group (CCG) risk management framework and sets out the systems, processes and accountability within the CCG for the reporting, investigation and management of all incidents and near misses, whether clinical, non clinical or of a serious nature including Serious Incidents (SIs) and any required external notifications. By adopting this policy, the CCG aims to improve the organisation's ability to:

- commission high quality, safe and accountable health services,
- minimise risk to patients and members of the public and
- ensure a safe working environment for staff whilst maximising the resources available.

2.0 Introduction

2.1 As a commissioner, the CCG procures a range of services some of which are large and complex. The CCG is committed to complying with legislation and NHS standards that require the CCG to have robust systems and processes in place for the reporting, investigation and management of all incidents and near misses which occur as part of the day to day organisational business.

As an NHS commissioning organisation, the CCG aims to learn and share the lessons learnt and improve its internal systems and processes, which underpin and support its statutory organisational and commissioning responsibilities. By adopting this approach, the CCG will greatly improve its ability to commission high quality patient care, ensure a safe environment for staff and effectively utilise its resources.

The CCG recognises that incident reporting is a fundamental tool of risk management in that it provides an opportunity to collect vital information about incidents to gain a better understanding of the underlying factors, system failures, errors or events that have occurred or had the potential to occur causing harm, loss, injury or damage.

2.2 The CCG adopts and upholds a 'fair blame culture' that encourages organisational learning and openness from errors, incidents or near misses to identify system failures and not to apportion blame. However, the CCG wishes to make it clear that incident reporting will not result in disciplinary proceedings save in exceptional circumstances such as:

- If there has been criminal negligence or criminal actions.
- Events so severe as to require an external inquiry.
- A staff member disregards established procedures.
- Failure to report a serious incident knowingly.

The CCG endeavours to improve its commissioning by embedding risk management and incident reporting into all areas of its business functions to ensure that lessons learnt lead to improvements within its commissioned health care services and/or organisational functions.

2.3 The CCG and all providers commissioned by the CCG will work in line with national requirements set out in the National Framework for Reporting and Learning from Serious Incidents Requiring Investigation (March 2010) and the NHS England Serious Incident Framework 2013 (http://www.england.nhs.uk/wp-content/uploads/2013/03/sif-guide.pdf)

The CCG is required to report all internal SIs to NHS England. All providers including non-NHS providers are expected to report all serious incidents (including Never Events, and serious health-care associated infections) directly to their commissioners including any organisation or person that is accountable to the CCG through contracting and commissioning arrangements.

3.0 Purpose

3.1 The purpose of this policy is to ensure that all members, staff and/or employees working for or on behalf of the CCG are aware of their duties when reporting, investigating or managing incidents.

It applies to all incidents whether they involve commissioned services, patients, carers, visitors, staff or members of the public and include property, premises, assets, information or any other aspect of the organisations business.

It gives direction and organisational regulation so that managers are aware of their duties in the approval, management and investigation of incidents and key personnel are aware of their duties of reporting incidents to external bodies as appropriate.

This policy aims to:

1. Ensure that all staff respond and learn from incidents.
2. Ensure that all incidents are reported in a timely manner.
3. Ensure that all staff contribute to the identification of risk, by reporting incidents and near misses, thus allowing preventative controls to be put in place.
4. Ensure that all SIs are investigated in a timely, efficient and effective way.
5. Ensure compliance with national reporting requirements.
6. Ensure the CCG has an open and honest approach to provider incidents affecting patients/relatives/carers, and a commitment to sharing lessons learned.
7. Ensure lessons learned from incidents and trends are shared across the organisation and fully acted upon by commissioned providers.
8. Enhance learning and development through the application of good performance management principles.

4.0 Responsibilities

4.1 Accountable Officer

The Accountable Officer has overarching responsibility for internal governance arrangements and managing providers responses to SIs and where appropriate for commissioning and co-ordinating SI investigations.

4.2 CCG Board

The CCG Board has overall responsibility for risk management and health and safety within the CCG. Through the reports and minutes from delegated sub-committees, the CCG Board must gain assurance that the process of incidents, complaints and claims investigations, and the learning and application of lessons learned, is working efficiently and effectively.

The CCG Board also receives quality and performance reports regarding all provider SIs, trends, and lessons learnt to ensure organisational learning and to prevent recurrence. It receives a summary of Grade 2 investigations, with recommendations and actions in the confidential section of its meeting.

4.3 The CCG Committee with Responsibility for Quality

The CCG Board has established a sub-committee that reports to it and has delegated responsibility for:

- Reviewing statistical evidence for all reported CCG Incidents, SIs, complaints, PALS and claims on a 6 monthly basis.
- Interpreting this data for trends analysis and assurance.
- Monitoring the feedback from external agencies on the incident reporting process.
- Ensuring all high and moderate graded incidents have an investigation completed within 30 days. This will be provided via the compliance report.
- Seeking assurance that the operational management of incidents within the CCG is both effective and efficient.

The Committee with responsibility for quality receives quarterly summaries of the provider organisation’s SIs, action plans, monitoring arrangements, and lessons learned and receives assurance from the provider that the action taken to investigate the SI and to prevent future occurrences is appropriate, robust and in line with the policy.

4.4 The CCG Clinical Lead with Responsibility for Quality

The Clinical Lead has corporate responsibility for the managing of the provider’s responses to SIs and for ensuring that Manchester CCGs have arrangements in place for managing the process of reporting and investigating SIs through STEIS within NHS provider services for which it is the co-ordinating commissioner. These arrangements include the grading of the incident, the quality of reporting, closure and monitoring the implementation of any action plans that arise from the SI.

4.5 Senior Management Team

It is the duty of all senior managers to ensure that all their staff comply with the incident reporting process and all of its associated procedures, and take appropriate action if this does not occur.

4.6 The Shared Corporate Services Team

The Corporate Services Team have the responsibility to:

- Ensure all staff using the Datix system are trained appropriately
- Implement this policy when appropriate for all internal serious incidents
- Inform the appropriate CCG lead and CCG Board or relevant Committee of reported incidents according to their significance
- Inform all relevant external bodies of a SI if appropriate in accordance with their requirements
- Ensure lessons are learned across the organisation and by educating staff
- Ensure that incident data collection is complete and appropriate
- Inform the CCG Board and/or relevant sub-Committee of reported incidents according to their significance
- Inform NHS England in accordance with their incident reporting requirements
- Provide reports to relevant CCG Board sub-committees or groups
- Undertake quarterly analysis of aggregated incident data for inclusion in the Quarterly Analysis Report
- Ensure lessons are learned across the organisation
- Inform all external agencies of incidents as statutorily obliged.

4.7 The Shared Performance and Quality Team

The Shared Performance and Quality Team has responsibility for managing the process that ensures that all commissioned providers are reporting, investigating, and taking action on provider incidents in line with this policy.

4.8 Line Managers (Incident Approvers and Investigators)

- Must take immediate action to prevent recurrence of an incident
- Ensure that the Datix incident form is completed for all incidents
- Ensure local investigations are carried out to a satisfactory and prompt conclusion; upload findings, action plans and documentation relevant to the investigation
- Retain all appropriate records, materials and equipment involved in the incident
- Maintain all records on the Datix incident reporting system
- Comply with this Policy and its reporting and management procedures
- Must inform their Senior Manager verbally, as soon as they become

aware, of a serious incident

- Must work with staff to take immediate action to prevent recurrence of any serious incident

4.9 **All Staff**

- Must comply with this policy and its reporting procedures and take all reasonable steps to minimise risks associated with incidents they report
- Must inform their line manager verbally as soon as they become aware of a SI
- Take all reasonable steps to minimise risks following an incident and assist with any incident investigation
- Retain all appropriate records, materials and equipment involved in an incident
- Assist with any incident investigation such as providing written statements on request of an investigation manager.

4.10 **Duties of commissioned organisations**

All service providers have a requirement to report, investigate and monitor incidents (including serious incidents) as specified within contracts and legislation.

5.0 Definitions of Terms Used

5.1 **Accident** – An unintentional event which can, but not always, cause harm.

Being Open - Open communication of patient safety incidents that result in harm or the death of a patient while receiving healthcare.

[Clinical] Governance - A framework through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which excellence in clinical care will flourish.

Culture - Learned attitudes, beliefs and values that define a group or groups of people.

Departments – Those working within the Manchester city wide teams to support the commissioning roles and responsibilities of the CCG.

Employee – An individual employed by the CCG directly or working on behalf of the CCG through a third party for a specific piece of work on a short/ medium term basis.

Hazard - Has the potential of something to cause harm to people or property.

Near Miss - A situation during any activity that fails to develop further, whether or not, as the result of intervening action, but carried with it, the potential to cause harm (i.e. “it almost happened”).

Incident - An event or circumstance that could have or did result in a member of staff/patient/member of the public suffering an unexpected death, major permanent harm or serious injury (or risk of serious injury), including health care associated infections, either where health services are provided or whilst in receipt of health care, or where actions of health service staff are likely to cause significant public concern.

Investigation - The act or process of investigating – a detailed enquiry or systematic examination.

Never Event - A serious, largely preventable, patient safety incident that should not occur if the available preventative measures have been implemented. The Department of Health (DoH) offers guidance on what constitutes a ‘Never Event’ and CCGs are required to monitor their occurrence within the services they commission.

Risk - The chance of something happening that will have an impact on individuals and/or organisations. It is measured in terms of likelihood and consequences.

Risk Assessment – The evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised.

Risk Management – All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

Risk Summit - A meeting of high-level leaders called to shape a programme of action, which is focused on sharing information willingly to help achieve a consensus about the situation under scrutiny and the actions required to mitigate the identified risks.

Root Cause Analysis (RCA) - A systematic process whereby the factors that contributed to an incident are identified. As an investigation technique for patient safety incidents, it looks beyond the individuals concerned and seeks to understand the underlying causes and environmental context in which an incident happened.

Serious Incident - A serious incident requiring investigation is defined as an incident that occurred in relation to NHS-funded services and care resulting in one of the following:

- unexpected or avoidable death of one or more patients, staff, visitors or members of the public;
- serious harm to one or more patients, staff, visitors or members of the public or where the outcome requires life-saving intervention, major surgical/medical intervention, permanent harm or will shorten life expectancy or result in prolonged pain or psychological harm (this includes incidents graded under the NPSA definition of severe harm);

- a scenario that prevents or threatens to prevent a provider organisation's ability to continue to deliver healthcare services, for example, actual or potential loss of personal/organisational information, damage to property, reputation or the environment, IT failure or incidents in population programmes like screening and immunisation where harm potentially may extend to a large population;
- allegations of abuse;
- adverse media coverage or public concern about the organisation or the wider NHS;
- one of the core set of never events.

6.0 Process for Reporting Internal Incidents

6.1 Incident reporting is a key element to promoting a safe culture and is a cornerstone of the wider risk management process within the CCG. An incident is any event that occurs or has the potential to occur which causes harm, injury, loss or damage to a patient, member of staff, or the CCG as an organisation.

In general all employees must report:

- Something that has happened that is contrary to the CCG's accepted standards of practice;
- An accident in which an employee, contractor or member of the public has been, or could have been, injured;
- An incident that places, or has placed employees, contractors, patients or visitors at unnecessary risk;
- An incident that could put the CCG in an adverse legal or an adverse media interest position.

6.2 All incidents must be reported by employees using the CCG's Datix electronic incident reporting system. Incident reporting must be undertaken in an accurate and consistent way, which will enable departments and management to action appropriately.

6.3 When completing the Datix incident form, it must be remembered that only factual statements must be made. Opinions must be omitted. Further guidance is available in Appendix A and a working example is available through the online Datix training tool.

6.4 All incidents reported to, or discovered by an employee, regardless of type or source should always be reported using the online Datix reporting form or if unavailable via the paper incident form (see Appendix D).

Types of incident include:-

Health and Safety Incident:
An unplanned and uncontrolled event that has led to or could have caused injury, ill health, harm to persons, damage to equipment or loss. Examples of Health and Safety incidents and actions required are:

- Accident: Where injuries have been sustained from an incident in the workplace (e.g. slip, trip, fall, etc.);
- Buildings Incident: Where an incident occurs due to defects and failures in estates and facilities.

Occupational Health:
Any health compromise or illness directly work-related (e.g. Sharps injury, latex allergy, stress, disease, unsafe exposure to substances hazardous to health, infection control/inoculation, poisoning, physical injury, etc).

Violence/Abuse/Discrimination:
Where any person is subject to the threat of, or to actual violence and/or verbal abuse or discrimination; the CCG is committed to the NHS Zero Tolerance Policy and encourages the reporting of these as a consequence.

Fire Incident:
Any incident involving a fire or any incident where the fire alarm sounds – including false alarms. Such incidents must also be reported to the CCG Fire Safety Officer, Senior Management and NHS Property Management Services as soon as possible after the incident has occurred.

Security or Data Security (i.e. Information Governance) Incident:
Any incident where a breach or a lapse of security or information governance is the dominating factor, e.g. theft or vandalism, premises window left open overnight, or data security incident, e.g. theft of a PC or potential/inadvertent or unauthorised disclosure of patient identifiable information.

(Further guidance for information governance incidents can be found in Appendix D)

Clinical/Patient Safety Incident:
Any unintended or unexpected incident that could have or did lead to harm (e.g. injury, suffering, disability or death – physical, psychological or social) for one or more persons receiving CCG commissioned/NHS-funded health care, (e.g. an occurrence, procedure or intervention, which has or could have given rise to actual injury, or to an unexpected or unwanted effect).

Events of Media Interest
If events cause media interest or have the potential to cause media interest.

7.0 Process for Managing Internal Incidents

7.1 When approving an incident, the following steps must be taken:

- Approvers must decide what local action will follow the incident:
  1. Green/Yellow graded incidents - no further action required, although a local investigation is required to take place and be included in the text of the initial incident report stating what immediate and or remedial actions have been taken.
  2. Orange/Red – local investigation must take place, findings and action

plans must be recorded on the incident system. Escalation may be needed if this is a particularly serious incident, meets SI criteria, or requires reporting to external agencies (see relevant section of this policy).

3. Action Plans must be updated until complete for all Orange and Red graded incidents, using the actions section of the incident reporting system.

- If an investigation falls outside the local approver's managerial responsibility then communication with the Corporate Services Team must take place to request an investigation by another area. This must be undertaken by using the communication/ feedback section of the incident reporting system.

- The approver must ensure that all parts of the incident report form have been completed **legibly** and review the risk grading criteria before the form is approved. Incidents must be graded according to the grading criteria outlined in Appendix B.

7.2 If an incident report form is duplicated local approvers should reject additional copies and note the reason for rejection in the appropriate box. If an incident report is produced inappropriately, they must be rejected and the employee informed of the correct procedures to follow. Please note that if an incident is 'rejected' on the Datix system a record of it will still be maintained.

7.3 Where an incident has occurred and action has been taken to address the immediate issues, should further actions be required to prevent future recurrence, further remedial action must be taken and recorded in the investigation section of the Datix incident reporting form regardless of the incident grading. Where there is difficulty or doubt about preventative action, this must be discussed with a member of the senior management team or the corporate services team. Further guidance can be found in Appendix C.

8.0 Process for Investigating Internal Incidents

8.1 As already mentioned earlier in this policy, all incidents graded orange or red must receive a formal investigation, which is recorded in the Datix system.

8.2 When investigating an incident one or more of the following must be included and documented:

- Identify system failures/causes that led to the incident.
- Identify corrective action required to prevent further recurrence or harm.
- Where appropriate obtain written statements from any persons involved in the incident or those who witnessed the incident (notes from interviews conducted and written statements must be uploaded into the documents section of the incident reporting system).
- Action plans must be added into the 'Action' section of the incident reporting system, with details of the responsible person to implement the action and due dates. This must then be updated and monitored by

the approver.

- Retain all records and documents relevant to the incident.
- Keep the staff informed at all times during the investigation and implementation of action plans.

8.3 On completion of an investigation the investigating manager should:

- Provide verbal feedback to personnel involved in the incident.
- Ensure original documentation gathered during the investigation has been uploaded into the 'Documents' section of the incident report form.
- Ensure the Datix system is updated with investigation findings and action plans.
- Ensure actions are implemented and monitored within agreed timescales.
- Consider wider sharing of the investigation outcome to ensure lessons are learned at team meetings, governance committee or for inclusion in CCG reports.

Further guidance can be found in Appendix C.

9.0 Process for Managing Internal (CCG) Serious Incidents

9.1 Serious Incidents

A degree of judgement is required when deciding to treat an incident as a SI and implement the SI procedure. A first indicator is when an incident has been graded as Red on the Datix system. Other indicators would be:

- Any incident that is reportable to NHS England – as per their Serious Incident Framework (http://www.england.nhs.uk/wp-content/uploads/2013/03/sif-guide.pdf)
- A death or life threatening event involving an employee, visitor, contractor or other persons on CCG premises or conducting CCG work
- Any incident which exposes the CCG, its employees or assets to potential or actual litigation
- Any incidents significantly damaging to the reputation of the CGG, its employees or assets
- Any major information governance incident or counter fraud incident (any major breach of corporate policies).

In devising the SI procedure (as recommended by the Redfern Report) the CCG has noted that depending on the nature of the SI, it may consider the need for a serious incident team (SIT) independent of the organisation to investigate.

Some SIs straddle other organisations. Therefore it may be necessary to undertake joint SI Investigations or to ensure that other organisations are aware and updated on the CCG's investigation and its findings and safety lessons are shared.

9.2 Central Reporting of a Serious Incident

Where a Serious Incident has occurred and been submitted on Datix, employees must not assume the incident report has been reviewed by the Corporate Services Department or senior management and must make a verbal report of the incident. If there is any doubt a telephone call must be made for advice and support.

Where an incident occurs out of hours, then the senior manager on call must be contacted who will provide assistance in actioning the incident and reporting the event to the Corporate Services Department when normal hours resume.

9.3 Serious Incident Reporting Procedure

The immediate priority in the case of SIs is to take steps necessary to secure the safety of CCG employees and other persons that may be involved in the incident. Subsequently, SIs should be reported and actioned as follows:

1. The Corporate Governance Manager or Head of Corporate Services (Monday to Friday during office hours) will inform the CCG Executive Leads or Accountable Officer immediately of any event and jointly take any remedial action necessary. The on-call Senior Manager (out of hours) will take any immediate remedial action necessary and inform the Corporate Governance Manager or Head of Corporate Services when normal office hours resume.

2. Comments or responses to the press or other media enquiries must only occur following discussion with the Head of Corporate Services and only after any patients, relatives or employees have been informed.

3. NHS England will be advised of the nature of the SI and that an investigation has commenced as soon as the SI is known and no later than 72 hours of knowledge of the SI. The final report will be submitted following completion of the investigation and no later than 45 working days following notification, unless unavoidable delays occur which must be discussed with NHS England. All reporting will be completed by reporting on the STEIS Serious Incident Reporting System and by telephone in accordance with the NHS England Serious Incident Reporting Protocol.

4. A SIT will be convened comprising of:
   - A CCG Senior Manager
   - Corporate Governance Manager or Head of Corporate Services
   - Lead Manager (of affected area/department)
   - Specialists as required (such as communications, information governance, counter fraud etc)

   The membership of the Team will be increased to include representation from the areas affected, according to the nature of the incident.

5. The principle functions of the SIT are:
   - Investigation of the SI to identify, as rapidly as possible, the facts and consequences, using RCA methodology. A timeline will be produced based on the SI and if necessary written statements gained.
   - Co-ordinate information, communication and press coverage as well as establishing efficient means of dealing with enquiries from press, media, relatives and members of the public.
   - Organise appropriate counselling and support for employees affected by the SI.
   - Production of an action plan designed to correct or limit the consequences, minimise the chance of recurrence in the future and allow lessons to be learned.
   - Production of a preliminary and final written report in a timely fashion under the guidelines set out in this document.

6. An investigating officer (Lead Investigator) must be appointed to manage the investigation, gather the facts of the SI, co-ordinate all statements and documentation, keep contemporaneous notes of the investigation meetings and ensure that the timescales set out in this policy are adhered to.

7. Consideration will be given as to whether it is appropriate to report the SI to the relevant professional or statutory body (e.g. Nursing and Midwifery Council, General Medical Council, General Dental Council, Health and Safety Executive, Medicine and Healthcare Related Products Agency or National Patient Safety Agency) including the outcome of the SIT investigation.

10.0 Process for Managing External (Provider) Serious Incidents

10.1 Procedure for Managing Provider Serious Incidents

The principle accountability of all providers is to patients and their carers/families. This means that the first consideration following an SI must be the patient's welfare. They must be cared for, their health and welfare secured, and they must be fully involved in the response to the SI. Where a patient has died or suffered serious harm, their family must be similarly cared for and involved.

Additionally, organisational accountabilities will underpin the response to SIs. Providers are accountable via contracts to their commissioners. The key organisational accountability for SI management is therefore from the provider in question to the commissioner.

The system is regulated by the Care Quality Commission (CQC).

10.2 Duties of organisations commissioned by the CCG to provide health

services

All service providers commissioned by the CCG, either as a co-ordinating commissioner or associate, have a requirement to report, investigate and monitor incidents (including SIs) as specified within contracts and legislation.

There are standardised NHS contracts for all service providers; the type of contract varies in relation to the size and function of the service provider. Within these contracts the requirement for the reporting, investigation and monitoring of incidents (including SIs) are outlined.

As detailed within all standardised NHS contracts and explicit within legislation all service providers are required to report SIs to their lead CCG and to co-operate fully with any investigation (as directed by the CCG/NHS England).

The CCG procedure for the monitoring and performance management of incidents (including SIs) within providers is attached as a schedule to all contracts the CCG holds with its service providers.

11.0 Process for Managing External Mental Health (City Wide) Serious Incidents

11.1 Procedure for Managing Provider Serious Incidents

Mental Health services for Manchester patients are commissioned through a Citywide Commissioning, Quality and Safeguarding Team (Citywide Team). All incidents reported by providers of these services are reviewed and monitored by the Citywide Team.

The principle accountability of mental health providers is to patients and their carers/families with wider considerations of others who may be affected. They must be cared for, their health and welfare secured, and the patient and their relative (as appropriate) must be fully involved in the review of the SI.

Incidents are managed as per the guidance in the NHS England Serious Incident Framework at http://www.england.nhs.uk/wp-content/uploads/2013/03/sif-guide.pdf)

Additionally, organisational accountabilities will underpin the response to SIs. Providers are accountable via contracts to their commissioners. The key organisational accountability for SI management is therefore from the provider in question to the commissioner.

The system is regulated by the Care Quality Commission (CQC).

11.2 Duties of Organisations commissioned by the CCG to provide Mental Health Services

All service providers are required to report, investigate and monitor incidents (including SIs) as specified within their contracts and legislation.

There are standardised NHS contracts for all service providers; the type of contract varies in relation to the size and function of the service provider. Within these contracts the requirements for the reporting, investigation and monitoring of incidents (including SIs) are outlined.

As detailed within all standardised NHS contracts and explicit within legislation all service providers are required to report SIs to their lead CCG and to co-operate fully with any investigation (as directed by the CCG/NHS England).

The CCG procedure for the monitoring and performance management of incidents (including SIs) within providers is attached as a schedule to all contracts.

12.0 Reporting to External Agencies

12.1 The CCG is responsible for ensuring incidents are reported in a timely manner to external agencies as detailed below and that safety lessons are shared.

12.2 **Police** - Incidents must be reported to the Police promptly when there is

- Evidence or suspicion of criminal activity;
- Evidence or suspicion that the actions leading to the incident were intended (such as fraud).

The CCG Accountable Officer should always be consulted before the police are called.

12.3 **NHS England** – CCG SIs will be reported to NHS England by the Corporate Services Team via the electronic STEIS system. Investigation reports will be shared with NHS England on completion of the investigation and within their timescales of 45 working days (unless otherwise stated by NHS England). If this is not possible, NHS England should be notified as soon as possible including reasons for any delay.

12.4 **Health and Safety Executive** (HSE) - Many incidents will be reportable to the HSE under the “Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)”.

The following are examples of reportable incidents under RIDDOR:

- Incidents which result in an employee or a self-employed person (working for the CCG) dying, suffering a major injury, or being absent from work or unable to perform their normal duties for more than seven days.
- Incidents which result in any person suffering an injury and being taken to hospital.
- An employee or self-employed person suffering from a work related disease, such as asbestos exposure.

The Corporate Services Team on receipt or further investigation of an incident report will undertake reporting to the HSE.

12.5 **Medicines and Healthcare products Regulatory Agency** (MHRA) – If the CCG receives any information from members or providers involving a medical device or medication which gives rise to, or has the potential to produce unexpected or unwanted effects involving the safety of patients, users or other persons, such incidents will be reported, by the CCG and providers to the Medicines and Healthcare Products Regulatory Agency (MHRA) when they did or could have led to:

- Death, life threatening illness or injury
- Deterioration in health
- The necessity for medical or surgical intervention
- Unreliable tests results leading to inappropriate diagnosis or treatment.

13.0 Process for Approval & Ratification

13.1 This policy will be approved and ratified at the CCG Board or sub-committee with responsibility for Quality, as a delegated committee of the Board with the right to approve policies as stated within its terms of reference.

14.0 Dissemination, Training & Advice

14.1 Once ratified this policy will supersede all previous incident reporting policies and procedures. In order that this policy is disseminated and implemented correctly the following will occur after ratification:

- The policy will be published on the CCG website and relevant links sent out via the communications and engagement department.
- Manchester Matters will include a link to this policy.
- The Datix risk management training is designed to match this policy and attendees are made aware of this policy.
- Senior managers will make their staff aware of this policy when questioned about incidents.
- Advice can be sought from the Corporate Services Team.

15.0 Review, Monitoring and Compliance

15.1 The policy will be reviewed every 3 years unless there is a significant change in legislation or process which requires an urgent change in procedure.

15.2 Monthly compliance monitoring reports will be produced by the Corporate Services Team for review, action and monitoring by the CCG Board or Committee with delegated responsibility for Governance. The report will record who is reporting incidents, the timeframe for approving incidents, outstanding investigations and reporting to external bodies. This will enable the Committee to be assured that incidents are being effectively and efficiently managed and investigated within the CCG, as statutorily required.

15.3 The incidents, complaints and claims report will be sent to the CCG Board or Committee with delegated responsibility on a quarterly basis. The report takes a holistic look at the information to identify providers and/or issues that the CCG should be considering and taking action on so that this can provide the

Committee with the assurance that trends within this data are being managed appropriately.

15.4 The reporting structure for incidents is outlines below:

Committee	Report Title	Report Details	Timeframes
Board	Governance Overview Report	Update from the Governance Committee – for assurance	Every Meeting
Quality Committee	Incident, Complaints and Claims Report	Analysis of all incidents, complaints and claims	Quarterly
	Internal Serious Untoward Incidents	All internal SUIs	As Required
Governance Committee	Compliance Report	Details reporting, approving and outstanding incidents.	Every Meeting

15.5 Monitoring Internal (CCG) Serious Incidents Process

All serious incident reports will be sent to the CCG Board or delegate Committee for review, comment and action. They will be sent again once the action plan is complete so the committee can seek assurance.

The incident complaints and claims report will be sent to the CCG Board or delegate Committee. The report takes a holistic look at all incidents, which may lead to serious incidents, complaints and claims, and gives the committee assurance that trends within this data are being managed appropriately.

15.6 Monitoring External (Acute Provider) Serious Incidents Process

The Clinical Lead with the responsibility for Quality will maintain the policy in conjunction with the Shared Performance and Quality Team

The effectiveness of this policy will be monitored by routine reporting, actions taken and other aspects of the service by the CCG's Committee responsible for Quality.

15.7 Monitoring External (Mental Health Provider) Serious Incidents

Incidents reported by Mental Health Providers will be monitored by the Citywide Commissioning, Quality and Safeguarding Team. Where possible a member of the team will attend the investigation meetings and seek assurance on actions taken and planned.

Incidents logged by providers will be reported via the Citywide Patient Safety Committee for review and agreement of closure on StEIS.

16.0 References

16.1 Legislation

- Health and Social Care Act 2012
- Health Act 2006
- Health and Safety at Work Act 1974
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
- The Management of Health and Safety at Work Regulations 1999 (a)
- The Corporate Manslaughter and Corporate Homicide Act 2007

16.2 Guidance

- NHS England (March 2013) Serious Incident Reporting Framework 2013
- National Patient Safety Agency (March 2010), National Framework for Reporting and Learning from Serious Incidents Requiring Investigation
- National Health Service Litigation Authority (NHSLA) Risk Management Standards
- Health and Safety Executive Documentation
- Management of Health and Safety at Work Regulations 1999
- Reporting of Incidents, Diseases and Dangerous Occurrence Regulations 1995
- The Mid Staffordshire NHS Foundation Trust Public Inquiry (Francis Report, 2013)
- Department of Health (2000) “An Organisation with a Memory: Report of an Expert Group on Learning from Adverse Events in the NHS”
- Secretary for State Directions - Protection of lone workers on accordance with the directions of health bodies on the measures to deal with violence against NHS staff and directions to health bodies on security management measures 2003 /2004 as amended in 2006.
- NHS Security Management Services 2009 - A guide for the better protection of lone workers in the NHS
- The NHS Code of Conduct for Managers (2007 and 2012)
- Organisation with Memory: Building a Safer NHS (2001)
- A promise to learn – a commitment to act: improving the safety of patients in England (Berwick Report, 2013)

16. 3 Policies

- Risk Management Framework
- Patient Services Policy (including Claims, Complaints and PALS)
- Anti-fraud, Bribery and Corruption Policy
- Disciplinary Policy

Appendix A – Guidance for Employees and Contractors

Any member of CCG staff can report an incident. Please remember to report an incident as soon as possible after the event. Access the DATIX incident form via the CCG Intranet page. A new Datix form will appear. Note: Mandatory fields are denoted by * and must be completed.

The Incident Form consists of nine sections and should be completed in line with the guidance below:

Incident Date and Time:

- On clicking the calendar button, a calendar will appear in the top left-hand corner of the screen. Click on the appropriate date to select.
- Although time is not a mandatory field, if you know the time please complete as this enables us to see if there are patterns and trends occurring at particular times of the day. (Please use 24-hour clock).

Incident Type:

- Please select the relevant 'type' of incident. Such as CCG incident or GP quality issue (the latter are likely to be issues that practices have made the CCG aware of).
- Select who was affected by the incident.

Details of Incident:

- Select the *service and location* of the incident (this may be the building and exact location for CCG incidents, such as 'Parkway Ground' – 'Kitchen').
- *Description of Incident* - Patient and staff identifiers must not be entered in these free text boxes. The words 'patient' or the staff members 'job title' should be used instead of names/unit numbers, to identify individuals. The description of the incident should be as detailed as possible, but based on facts only, personal opinion must be avoided at all times.
- *Immediate Action Taken* - Patient and staff identifiers must not be used. Details of actions taken following the incident must be reported based on fact, personal opinions must be avoided.

Incident Coding:

- Using the pull down menus select the most appropriate category and sub category to describe the incident (if you are unable to find the appropriate code please select the next most appropriate or contact the Corporate Services Team for guidance).

Incident Result and Severity:

- Indicate in the Result box whether the incident resulted in harm, no harm or was a near miss.
- Indicate in the Severity box the degree of harm that was caused.

Documents:

- You can upload any documents that were of relevance to the incident in this section. This is particularly helpful for investigating incidents.

Details of the person reporting the incident:

- This section is to record your details in case we need to follow up on the information provided or during an investigation. You should provide your work contact details, including your NHS email address, which is used to acknowledge the incident form has been sent appropriately.

Reporters Location:

- From the drop down boxes please select the location you are reporting the incident from. This is usually the department in which you work.

Responsible Manager:

- Choose your managers name from the drop down box. (if you are unable to find the your manager please select the next most appropriate person or contact the Corporate Services Team for guidance)

Completion of Incident Report:
When the form is complete, click ‘submit incident’ at the bottom of the page. The form will not submit if any mandatory information is missing and a prompt will appear. An incident number will be generated which can be noted for future reference and used for requesting feedback. Additionally, the reporter has the option to print a copy of the information submitted. The appropriate incident approvers will automatically be notified of the incident. You should still inform your local manager of the incident verbally.

Appendix B – Risk Grading

It is necessary to rate risk systematically using standard methodology, so that they can be placed into one of the three categories above. This allows prioritisation of remedial action. All incidents should be rated in 2 ways:

Assessment of Consequence

Choose the most appropriate domain for the identified risk from the left hand side of the table. Then work along the columns in the same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards

Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million

Service/business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Assessment of Likelihood of Reoccurrence

The tool described here provides a simple way of rating the potential risk associated with hazards. It requires an assessment of rating the potential consequences and the likelihood of recurrence of harm from the hazard. (A hazard is anything that has the potential to lead to or cause actual harm, the risk is how likely the hazard will cause harm).

Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur,possibly frequently

Risk Rating = Consequence X Likelihood

Measures of Consequence

Level	Descriptor	Description
1	Insignificant	No adverse outcome or injury
2	Minor	Short term adverse outcome
3	Moderate	Semi-permanent outcome or injury
4	Major	Permanent adverse outcome or Injury
5	Catastrophic	Death; Adverse Publicity etc

Measures of Likelihood of Reoccurrence

Level	Descriptor	Description
1	Rare	Can't reasonably believe that this will ever happen again
2	Unlikely	Do not expect it to happen again but it is possible
3	Possible	May re-occur. Occasionally
4	Likely	Will probably re-occur but is not a persistent issue
5	Almost certain	Likely to re-occur on many occasions, a persistent issue

Risk Grading Matrix

Likelihood	**Consequence**				
	Insignificant	Minor	Modorate	Major	Catastrophic
Rare	1	2	3	4	5
Unlikely	2	4	6	8	10
Possible	3	6	9	12	15
Likely	4	8	12	16	20

Appendix C – Guidance for Approvers and Investigators

Nominated managers review and approve incidents. All ‘approvers’ must have undertaken training in the reviewing of incidents. This can be accessed by contacting the Corporate Services Team. Access to the system is only provided once training is complete.

On submission of an incident an e-mail is automatically generated and sent to the nominated ‘approver’. The incident must be reviewed in a timely manner. A five-day time frame has been set from the date the incident was reported through to final approval. This time-scale will be performance managed by the Compliance Report that is presented to the CCG’s Governance Committee.

Approving and checking incidents:

The local approver must check that the following information is present, factual and accurate:

- What happened
- When it happened
- Where it happened
- Who/ what was involved
- What the outcome was and what immediate action was taken
- Ensure that staff/ patient names do not appear on the “description of incident” and the “immediate action taken”, if they do, the names should be deleted and replaced with generic terms
- Ensure that the description and action taken fields are factual accounts, and not those of opinion.
- Check category and sub category are correct for of coding
- Assign a grading and identify appropriate level of investigation. ***Note***: all orange and red incidents must be investigated formally within 30 days
- Look out for any patterns, trends or key issues
- Finally approve the incident and add a ‘closed date’.

The approver has the facility to add/amend information as necessary to any of the fields. Any changes made will appear on the audit trail.

- The feedback facility can be used to email reporting staff with feedback on the outcome of the incident or if further information is required. The CCG advises approvers to try and respond to all incident reporters and create a culture of 100% feedback from incident reporting.

If the incident requires investigation:

Approvers are responsible for identifying incidents in need of investigation. These will be monitored and performance managed by the Corporate Services Team.

1. Green/Yellow incidents = no further action, but should be monitored locally for trends
2. Orange incidents = must be Investigated at a local level
3. Red Incidents = Does this require an internal Serious Incident investigation/procedure?

Where the investigation is outside your normal management responsibilities you should use the communication and feedback section to inform the relevant investigator that another area needs to be completed.

Add lessons learned and further actions taken to the Investigation Section (which can be found on the left hand side of an incident form). Complete the investigator box, dates and costs where applicable as well as the “Lessons Learned” and “Actions taken” fields with as much detail as possible.

Complete the action plan with who is responsible for each action and the timeframes given for the action to be completed. These should include actions undertaken to prevent or reduce the likelihood of recurrence.

You must also ensure if further documentation has been produced as part of the investigation process you retrieve the incident form and attach documents e.g. RCA, C Diff, by clicking the document section and add a document.

Appendix D – Information Governance Incident Procedure

Information Governance Related Incident

An Information Governance or Information Security related incident relates to breaches of security and/or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street.
It could also be any event that has resulted or could result in:

- The integrity of an information system or data being put at risk;
- The availability of an information system or information being put at risk;
- An adverse impact, for example, embarrassment to the NHS, threat to personal safety or privacy, legal obligation or penalty, financial loss and/or disruption of activities.

Some more common areas of incidents are listed below but this list is not exhaustive and should be used as guidance only. If there is any doubt as to what you have found being an incident it is best to report it to the relevant person for this decision.

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness;
- Loss of computer media, for example, CDs, memory sticks/USB sticks due to crime or an individual's carelessness;
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident.

Breach of confidentiality

- Finding a computer printout with personal identifiable data on it in a public area;
- Finding any paper records about a patient/member of staff or business of the organisation in any location outside secured CCG premises;
- Being able to view patient records in an employee's car;
- Discussing patient and/or staff personal information with someone else in an open area where the conversation can be overheard;
- A fax being received by the incorrect recipient.

Information Governance Related Serious Incidents (SI)

There is no simple definition of an Information Governance incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious or vice versa. Please see the link below "Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation" document for further details and examples.

https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf

As a guide, any incident involving the actual or potential loss of personal information that could lead to identity fraud or have another significant impact on individuals should be considered as serious. This definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

Categorising of the incident assists to distinguish the severity level of the Information Governance related incident and whether it is a SI or not. This is explained in later sections of this procedure.

Process for Reporting Information Governance Incidents

Staff must follow the above policy in order to report any incident. All Information Security/Information Governance incidents must be reported using this procedure only and no other method.

On receipt of the Greater Manchester Commissioning Support Unit (GMCSU) IG Team being notified of incidents relating to Information Governance, the severity score is calculated according to the checklist contained within the "Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (SIRI's)" (Health and Social Care Information Centre, June 2013, Version 2). Please see link below Annex A:

https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf

This is then logged in the Information Governance Incidents Logbook managed by the GMCSU IG Team.

The GMCSU IG Team based at the CCG where the incident has occurred must be notified of all Information Governance/Information Security incidents as well as logging this following the CCG's incident reporting processes. The immediate response to the incident and the escalation process for reporting and investigating of incidents will vary according to the severity level of the incident.

IG Toolkit Incident Reporting Tool

Where it is suspected that an IG SIRI (Serious Incident Requiring Investigation) has taken place, this will be logged on the IG Toolkit Incident Reporting Tool. This is mandated from 1st June 2013. The IG Incident Reporting Tool which can be found on the IG Toolkit website will play a key role in providing visibility/knowledge and encouraging collaborative partnership working amongst key stakeholders to find solutions for addressing issues. Key staff will also be informally notified (Chief Operating Officer, Senior Information Risk Owner, Caldicott Guardian and/other Directors) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'.

Guidance on how to use the IG Incident Reporting Tool can be found by clicking the icon below:

https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf

StEIS will be used for reporting all SI's and initial report should be made as soon as possible. StEIS should be regularly updated as appropriate.

Assessing severity of Information Governance Incident

The IG SIRI's category is determined by the context, scale and sensitivity of the incident. Every incident is categorised at the following levels:

1. Confirmed IG SIRI but no need to report to the ICO, DH and other central bodies.
2. Confirmed IG SIRI that must be reported to ICO, DH and other central bodies.

A further category of IG SIRI is also possible and is to 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.

If an incident is found to have neither occurred or the severity of the category has been reduced due to factors that were not planned for the incident will be recorded as a "near miss". This will allow for the CCG to undertake a lessons learned exercise.

The following process is used to categorise an IG SIRI. This can also be found in the checklist guidance referenced earlier in this document.

Step 1

Any incident will need to have a baseline assessment which will allow the final score to be identified. To establish the baseline the incident must be scored using the table below:

Baseline Scale	
0	Information about less than 10 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 501-1000 individuals
3	Information about 1001-5000 individuals
3	Information about 5001-1000 individuals
3	Information about 1001-100,000 individuals
3	Information about 100,001+ individuals

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 to all key bodies notified.

Step 2

The below table will allow for the sensitivity characteristics to be scored and therefore permit the baseline score to be adjusted accordingly

Sensitivity Factors (SF)

Low:	For each of the following factors reduce the base line score by 1
-1 for each	No clinical data at risk
	Limited demographic data at risk e.g. address not included, name not included.
	Security controls/difficulty to access data partially mitigates risk.

Medium:	The following factors have no effect on the baseline score
0	Basic demographic data at risk e.g. equivalent to telephone directory.
	Limited clinical information at risk e.g. clinic attendance, ward handover sheet.

High:	For each of the following factors increase the baseline score by 1
+1 for each	Detailed clinical information at risk e.g. case notes
	Particularly sensitive information at risk e.g. HIV. STD, Mental Health, Children.
	One or more previous incidents of a similar type in the past 12 months.
	Failure to securely encrypt mobile technology or other obvious security failing.
	Celebrity involved or other newsworthy aspects of media interest.
	A complaint has been made to the information Commissioner.
	Individuals affected are likely to suffer significant distress or embarrassment.
	Individuals affected have been placed at risk of physical harm.
	Individuals affected may suffer significant detriment e.g, financial loss.
	Incident has incurred or risked incurring a clinical untoward incident.

Step 3

Where the adjusted score indicates that the incident is a level 2 or more, the incident will be reported to the ICO and the DH automatically via the IGT Incidents Reporting Tool.

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

As more information becomes available, the incident level should be re-assessed.

Where the level of likely media interest is initially assessed as minor but this assessment changes due to circumstances (e.g. a relevant FOI request or specific journalist interest) the SUI level should be revised as quickly as possible and all key bodies notified. Note that informing data subjects is likely to put an incident into the public/media domain.

5.0 Management and investigation of IG reported incidents

Incidents scored 0 - 1

For incidents that are scored 0 -1, senior members of staff in that area/department are responsible for the investigation of that incident and assessing the situation. The GMCSU IG Team located in the CCG will be there to provide support and guidance and provide any additional information or training that may be required. It is integral that any action taken is to minimise the potential adverse effects of the incident and help to minimise the risk of the incident occurring in the future as this could result in a SIRI.

Incidents scored 2+

For incidents that are scored 2 and above the following action should be undertaken in conjunction with the GMCSU IG Team within the CCG:

- Appoint an investigating Officer;
- Engage appropriate specialist help (IG, IT, Security, Records Management);
- Where across the organisational boundaries coordinate investigations and incident management;
- Carry out a RCA;
- Ensure that all relevant rules in regards to interviews, evidence and preservation of evidence are followed;
- Document investigation and findings;
- Ensure that content is reviewed;
- Identify lessons learned.

For all incidents it is important that the information that is held within the IG Incident Reporting Tool is relevant and up to date therefore the GMCSU IG Team for the CCG should be kept up to date of all developments. Please note that all information under a closed IG SIRI will be published quarterly by the Health and Social Care Information Centre. Therefore it is integral that all the information recorded is appropriate and does not include information that would not normally be released under the Freedom of Information Act 2000.

Appendix E – Equality Analysis

GMCSU Equality Analysis Form

The following questions will document the effect of your activity on equality, and demonstrate that you have paid due regard to the Public Sector Equality Duty. The Equality Analysis (EA) guidance should be used read before completing this form.

To be completed at the earliest stages of the activity and before any decision making and returned via email to GMCSU Equality Diversity Human Rights Team for Quality Assurance:

Samina Arfan: samina.arfan@nhs.net	**Andrew McCorkle:** andrew.mccorkle@nhs.net
Julia Allen: juliaallen@nhs.net	**Rosie Kingham:** rosie.kingham@nhs.net

	Section 1: Responsibility	**EDHR Reference :** **Your ref:**
1	Name & role of person completing the EA:	David Smith - Corporate Governance Manager
2	Service/ Corporate Area	Corporate Governance
3	Head of Service or Director (as appropriate):	Nick Gomm
4	Who is the EA for? Select from the drop down box.	Manchester Central CCG
4.1	Name of Other organisation if appropriate	All Manchester CCGs
	Section 2: Aims & Outcomes	
5	What is being proposed? Please give a brief description of the activity.	Incident Reporting Policy
6	Why is it needed? Please give a brief description of the activity.	Incident Reporting helps keep staff safe by reducing health and safety incidents. It is also a mandatory part of the CCG work to monitor incidents (especially serious incidents) from our providers.
7	What are the intended outcomes of the activity?	Lower risk to staff and organisation
8	Date of completion of analysis (and date of implementation if different). Please explain any difference	11/06/2014
9	Who does it affect? Select from the drop down box. If more than one group is affected, use the drop down box more than once.	CCG Staff
	Establishing Relevance to Equality & Human Rights	

10 **What is the relevance of the activity to the Public Sector Equality Duty? Select from the drop down box and provide a reason.**

General Public Sector Equality Duties	Relevance (Yes/No)	Reason for Relevance
To eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by Equality Act 2010	No	

	To advance equality of opportunity between people who share a protected characteristic and those who do not.	No	
	To foster good relations between people who share a protected characteristic and those who do not	No	

10.1 Use the drop down box and advise whether the activity has a positive or negative effect on any of the groups of people with protected equality characteristics and on Human Right

Protected Equality Characteristic	Positive (Yes/No)	Negative (Yes/No)	Explanation
Age	Yes		Reporting for all staff - also anonymous reporting available
Disability	Yes		
Gender	Yes		
Pregnancy or maternity	Yes		
Race	Yes		
Religion and belief	Yes		
Sexual Orientation	Yes		
Other vulnerable group	Yes		
Marriage or Civil Partnership	Yes		
Gender Reassignment	Yes		
Human Rights	Yes		

If you have answered No to all the questions above and in question 10, explain below why you feel your activity has no relevance to Equality and Human Rights.

Section 4: Equality Information and Engagement

11 What equality information or engagement with protected groups has been used or undertaken to inform the activity. Please provide details.

Details of Equality Information or Engagement with protected groups	Internet link if published & date last published
N/A	

11.1 Are there any information gaps, and if so how do you plan to address them	None

Section 5: Outcomes of Equality Analysis

12 Complete the questions below to conclude the EA.

	What will the likely overall effect of your activity be on equality?	
	What recommendations are in place to mitigate any negative effects identified in 10.1?	
	What opportunities have been identified for the activity to add value by advancing equality and/or foster good relations?	
	What steps are to be taken now in relation to the implementation of the activity?	
Section 6: Monitoring and Review		
13	If it is intended to proceed with the activity, please detail what monitoring arrangements (if appropriate) will be in place to monitor ongoing effects? Also state when the activity will be reviewed.	
	Monitoring every time the policy changes	