Lincolnshire East
Clinical Commissioning Group

Serious Incident Policy

Reporting and Investigation Guideline for Serious Incidents

Reference Number:	RM003
Version:	5.0
Name of Originator / Author & Organisation:	Federated Clinical Risk Management Team
Responsible LECCG Committee:	QPEC
LECCG Executive Lead:	Tracy Pilcher, Chief Nurse
Date Approved by LECCG Authorising Committee:	09.01.19
Review Date:	November 2021
Target Audience:	All CCG Staff; Commissioned Services
Distributed via:	Intranet Website
Date Policy Circulated:	16.01.19

NHS
Lincolnshire East
Clinical Commissioning Group

Serious Incident Policy

Reporting and Investigation Guideline for Serious Incidents

Version Control Sheet

Version	Section / Para / Annex	Version / Description of Amendments	Date	Author / Amended by
5.0	Personal Data Breaches (Data Security and Protection Incidents)	Updated section Personal Data Breaches (Data Security and Protection Incidents) to reflect most recent guidance.	21.11.18	Tracy Petch/ Kelly Huckle

Executive Summary

Serious Incident Policy

Background

NHS England published a revised Serious Incident Framework in 2015, together with an updated Never Events Policy and Framework. The revised Framework replaced the National Framework for reporting and Learning from Serious Incidents Requiring Investigation, issued by the NPSA in March 2010 and NHS England's Serious Incident Framework published in March 2015.

The NHS England Serious Incident Framework (2015) defines the fundamental purpose of patient safety investigation SIs to learn from incidents, not to apportion blame, whilst identifying a system-based method for conducting investigations (root cause analysis).

The CCG has a dual function in relation to serious incidents:

- Firstly, to receive notification of incidents, related to Lincolnshire residents, from provider Organisations, Reflecting the responsibilities of a Commissioner, the CCGs should ensure that all appropriate action has been undertaken by the notifying Organisation, to learn and share lessons, and promote public safety and confidence.

- Secondly, the CCG must ensure that Serious Incidents (SI's), relating to actions/services undertaken by the CCG, are identified, reported and managed in an effective and timely way.

The organisation where the incident occurred has overall responsibility for the investigation, the immediate dissemination of learning and the implementation of subsequent action plans.

Statement

The CCGs are committed to the timely and effective reporting and management of Serious Incidents, to promote patient and organisation safety.

CCG Responsibilities

The Accountable Officer of the CCG has ultimate responsibility for the Serious Incident reporting process for services commissioned by the CCG.

This responsibility is discharged through the CCG Executive Nurse & Quality Lead. Day to day management and oversight of the SI process is further delegated to the Head of Clinical Risk Management and Compliance within the Federated Clinical Risk Management Team.

All CCG employed staff must ensure that "Serious Incidents" are reported immediately to their Line Manager or, if not immediately available, to the Federated Clinical Risk Management team.

Staff working out of hours should report Serious Incidents and RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurences) incidents according to the guidance in this procedure.

Training

Training will be provided to the Organisation's employed staff through the CCG Induction Programme. This training will be supplemented for both clinical and non-clinical staff by mandatory training updates.

Dissemination

The policy will be available on the Organisation website.

Resource Implications

The successful implementation of incident reporting requires robust staff training and access to appropriate information systems and analytical tools.

S**erious Incident Policy**

Statement: Lincolnshire CCGs are committed to the commissioning of safe, effective and high quality healthcare. In order to support this, Lincolnshire CCGs expect the timely and effective reporting and management of serious incidents by Organisations where services are commissioned, to promote patient and organisation safety.

The Lincolnshire CCGs are also committed to the timely and effective reporting and management of their own serious incidents to promote and ensure patient, staff and organisation safety.

Background:
NHS England published a revised Serious Incident Framework in 2015, together with an updated Never Events Policy and Framework. The revised Framework replaced the National Framework for reporting and Learning from Serious Incidents Requiring Investigation, issued by the NPSA in March 2010 and NHS England's Serious Incident Framework published in March 2013.

The NHS England Serious Incident Framework (2015) defines the fundamental purpose of patient safety investigation sis to learn from incidents, not to apportion blame, whilst identifying a system-based method for conducting investigations (root cause analysis).

The CCG has a dual function in relation to serious incidents:

- Firstly, to receive notification of incidents, related to Lincolnshire residents, from provider Organisations, Reflecting the responsibilities of a Commissioner, the CCGs should ensure that all appropriate action has been undertaken by the notifying Organisation, to learn and share lessons, and promote public safety and confidence.

- Secondly, the CCG must ensure that Serious Incidents (SI's), relating to actions/services undertaken by the CCG, are identified, reported and managed in an effective and timely way.

The organisation where the incident occurred has overall responsibility for the investigation, the immediate dissemination of learning and the implementation of subsequent action plans.

Definition of a Serious Incident
The definition of a Serious Incident requiring investigation is set out in the NHS England Serious Incident Framework – Supporting Learning to Prevent Reoccurrence (March 2015). The Framework identifies serious incidents as events in healthcare where the potential for learning is so great, or the consequences to patients, families, carers, staff or organisations are so significant, that they warrant using additional resources to mount a comprehensive response.

In accordance with the NHS England Framework (March 2015), there is no definitive list of events/incidents that constitute a serious incident. The definitions below identify the circumstances in which a serious incident must be declared.

Serious incidents in relation to NHS include acts and/or omissions occurring as part of NHS funded healthcare (including in the community) that resulting in:
Unexpected or **avoidable** death of one or more patients, staff, visitors or members of the public. This includes suicide/self-inflicted death and homicide by a person in receipt of mental health care within the recent past (as a minimum the last 6 months).

Unexpected or avoidable injury to one or more people that has resulted in serious harm;

Unexpected or avoidable injury to one or more people that requires further treatment by a healthcare professional in order to prevent the death of the service user or serious harm.

Allegations of **abuse;** sexual abuse, physical abuse or psychological ill treatment, or acts of omission which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self - neglect, domestic abuse, human trafficking and modern day slavery where healthcare did not take appropriate action/intervention to safeguard against such abuse occurring; or where abuse occurred during the provision of NHS funded care.

- This includes abuse that results in (or was identified through) a Serious Case Review (SCR), Safeguarding Adult Review (SAR), Safeguarding Adult Enquiry or other externally-led investigation, where delivery of NHS funded care caused/contributed towards the incident. (see NHS England Serious Reporting Framework, March 2015 Part One Sections 1.3 and 1.5)

An incident (or series of incidents) that prevents, or threatens to prevent an organisation's ability to continue to deliver an acceptable quality of healthcare services, including (but not limited to)

- Failures in the security, integrity, accuracy or availability of information, often described as data loss and/or information governance related issues.
- Property damage
- Security breach/concern
- Incidents in population-wide healthcare activities like screening and immunization programmes where the potential for harm may extend to a large population
- Inappropriate enforcement/care under the Mental Health Act (1983) and the Mental Capacity Act (2005) including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS)
- Systematic failure to provide an acceptable standard of safe care (this may include incidents, series of incidents, which necessitate ward/unit closure or suspension of services or
- Activation of major incident plan (by provider, commissioner or relevant agency)

Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation.

A Never Event – all never events are defined as serious incidents although not all never events necessarily result in serious harm or death. See Never Events Policy and Framework for list of Never Events.

Never Events Policy/Framework available online at: http://www.england.nhs.uk/ourwork/patientsafety/never-events/

Near Misses may also be classed as a serious incident because it is acknowledged that the outcome of the incident may not reflect the potential severity of harm that could be caused should the incident occur again. An assessment of whether the near miss should be classified as a serious incident should be an assessment of risk considering:

- The likelihood of the incident occurring again if current systems/process remain unchanged
- The potential for harm to staff, patients and the organisation should the incident occur again

12 Hour Trolley Breaches reported as serious incidents in line with the Midlands and East 12 Hour Breach Reporting protocol issued in June 2015.

The Responsibilities

The Commissioner (Lincolnshire CCGs) will, as part of their commissioning role, performance monitor the contract in place with all its provider organisations, to ensure the continuous improvement in the provision of quality care. The Commissioners will receive notification of serious incidents identified by provider organisations; and quality assure the robustness of the serious incident investigations undertaken by the Provider. To include the provision and implementation of action plans developed in response to investigations undertaken.

The Commissioner will also ensure that an agreement is in place to work with other Commissioning Organisations where multiple commissioners commission services from the same provider.

The information received through serious incident notification/investigation will be utlised by the Commissioner to:

- Ensure, through positive challenge, that the processes and outcomes of investigations include identification and implementation of improvements to prevent reoccurrence of the serious incident; and sanction closure of the SI on STEIS when necessary assurance/action has been secured.
- Source specialist expert review of serious incident investigations where this is merited.
- Triangulate information gathered through serious incident investigations with other information and intelligence to inform actions to continuously improve services and inform future commissioning discussions
- Share intelligence, appropriately, with relevant regulatory and partner organisations i.e. through forums such as the local Quality Surveillance Group (QSG)

The Commissioner will also have a procedure in place for managing concerns raised in relation to the management of the investigation process.

Throughout the year, the Commissioners will produce and review at their Quarterly Quality and Patient Experience Committees (QPEC), quarterly reports on provider SIs. At the end of the financial year it is expected that CCG's will report to the public part of their Governing Body, the total number of never events and incidents of data loss for their Provider Organisations and/or their own CCG.

The Commissioner will also ensure the provision of performance reports on provider's provision of investigation reports within the 60 working day timescale, to the quarterly Quality Review Meetings (QRM).

In collaboration with Local Authorities, the Commissioner has responsibility for protecting public health by controlling communicable disease and infection. This responsibility is matched with a requirement for the Organisation to report and escalate incidents, in line with national and local policy.

The Commissioner will ensure that service level agreements established with the Provider Organisations with which it commissions, identify systems for reporting, monitoring and investigating a Serious Incident. This requirement includes Independent Providers and Care Homes, in those instances where the NHS is commissioning the care provided.

The Commissioner will additionally review and quality assures steps taken by external Provider Organisations to manage reported SIs. In complex situations, where multiple providers are involved etc. the CCGs will provide additional appropriate support as required to ensure the investigation process is progressed appropriately. This may include the requirement to access resources/expertise and access to competent independent investigators where independent investigation may be required.

The CCGs will report onto the STEIS system serious incidents reported by commissioned services who do not have access to the NHS STEIS system i.e. general practices and private healthcare providers commissioned to provide services to NHS patients etc.

The Commissioner will also have in place a process, identified within the SI Policy for the management of its own serious incidents reported.

Duties:

Accountable Officer

The CCG Accountable officer has ultimate responsibility for the Serious Incident reporting process within the Organisation, and management/monitoring of serious incident reporting/investigation of commissioned services.

.

CCG Executive Nurse for Quality and Patient Safety

The responsibility for the oversight of serious incident management and monitoring for the CCGs and commissioned services is delegated to the CCG Executive Lead Nurse for Quality and Patient Safety. (or delegated deputy)

The CCG Executive Lead Nurse for Quality and Patient Safety (or delegated deputy) is responsible for the closure of provider serious incident investigations through attendance at the Serious Incident group as required.

The CCG Executive Lead Nurse for Quality and Patient Safety (or delegated deputy) is responsible for ensuring the appropriate oversight, reporting, review and closure of serious incidents reported by general practice.

The CCG Executive Lead Nurse for Quality and Patient Safety (or delegated deputy) is responsible for receiving, risk assessing and managing the investigation and reporting of “own reported” SI’s on behalf of the CCG**,** and those incidents that relate to general practice

The management and strategic overview of the serious incident function for general practices resides with the CCG Executive Nurse Lead for Quality and Patient Safety, delegated to the CCG Quality Managers to manage on a day to day basis.

The Federated Clinical Risk Management Team

The Federated Clinical Risk Management Team is responsible for the day to day management of commissioned service serious incidents on behalf of the CCGs in Lincolnshire.

Whilst the CCG Executive Lead Nurse for Quality and Patient Safety is responsible for the management of any concerns relating to the management of the serious investigation process, day to day management of these concerns is delegated to the Head of Clinical Risk and Compliance within the Federated Clinical Risk Management Team.

The Federated Clinical Risk Management Team is responsible for ensuring that the appropriate notification is received by the Executive Lead Nurse for Quality and Patient Safety (and the appropriate deputy) of serious incidents relating to services for which they are a lead commissioner; or where the incident relates to a patient residing within their CCG area.

The Federated Clinical Risk Management Team is responsible for the risk assessment and performance management of all serious incidents reported via STEIS by provider organisations/CCGs. The Federated Clinical Risk Management Team will manage the Datix information system to support the monitoring of serious incidents reported; undertake trend analysis and provision of serious incident monitoring/management reports; secure assurance regarding actions taken to ensure patient safety following a serious incident and ensure the continued development of the SI management process on behalf of Commissioners, inclusive of the managed of the SI Review Group.

The Federated Clinical Risk Management Team is responsible for providing feedback to provider organisations regarding assurances, further actions and closures resulting from the review of the serious incident investigation reports received.

The Federated Clinical Risk Management Team is responsible for the updating of STEIS on behalf of the Commissioner.

The Federated Clinical Risk Management Team is responsible for updating the Datix and STEIS system on behalf of the CCGs for serious incidents relating to general practice and CCG staff.

The On Call Director

The On Call Director will receive notification of Provider SI's out of hours, respond to any immediate risk presented and inform the Federated Clinical Risk Management team of this action the next working day.

Investigation Managers

For the CCGs own serious incidents/general practice incidents, a nominated Root Cause Analysis (RCA) Investigation Manager(s) is responsible for leading the RCA for a SI. Investigation Managers will be selected for their specialist expertise, they will interview staff; collate and analyse evidence and write the final RCA report. An Investigation Manager for CCG 'own reported' SIs will be nominated by the CCG Executive Lead Nurse to complete a full RCA.

Employed (and sub contracted) staff are required to be familiar with the SI reporting policy and be able to identify and escalate incidents which fall within the SI criteria in accordance with this policy. Staff are responsible for reporting all SI incidents to their line manager and onward to the Federated Clinical Risk Management team. Staff are required to complete an incident report form via the online Datix System to provide a written audit trail. Staff have a responsibility to identify training needs in relation to the SI process, to their line manager. Staff who have line management responsibilities have the responsibility to consider and respond to training needs identified by their staff and to support their direct reports (in liaison with the CCG Executive Lead Nurse for Quality and Patient Safety) to report and manage risks related to a SI.
All staff members are encouraged to be Open (detail found within the Being Open Policy). Staff should also be familiar with the CCG Whistle Blowing process.

Serious incidents should be reported within 2 working days of the incident being identified.

Role of the Governing Body:
The Governing Body has executive oversight of Serious Incidents (SI's) reported in relation to the resident population.

The Governing Body will support a fair and open culture in the reporting and management of these incidents consistent with the principles of the national guidance, "Being open" and duty of candour. The Quality and Experience Committee as a sub-committee of the Governing Body will receive regular reports describing Serious Incidents, including assurance regarding action taken to mitigate risk and lessons learnt.

Role of the CCG Risk and Governance Committee:
The Risk and Governance Committee has over sight of risk which is inclusive of Serious Incidents, for the CCG, on behalf of the Organisation's Governing Body.

Role of the CCG Quality and Patient Experience Committee:
The CCG Quality and Patient Experience Committee's receive detailed reports describing SI incident themes and action. The Committee is responsible for critically evaluating this information, ensuring that all required action has been taken to respond to patient safety concerns highlighted, escalating where necessary both internally and external to the CCG and to the Regulator, should significant risk be identified.

Serious Incident (SI) Group:
The CCG are responsible for reviewing and closing SI's reported by Providers on the STEIS database when satisfied that an appropriate investigation has been undertaken, when lessons learnt have been identified and an appropriate action plan developed and implemented. This function is delegated to the Executive Lead Nurse for Quality and Patient Safety and operationalised through the SI group.

The serious incident (SI) Group will meet on a monthly basis to review serious incidents submitted by provider organisations. Additional serious incident group meetings may be identified should the level of investigation reports received, merit additional review meetings being held.

Responsibilities of NHS Provider Organisations:

Provider Organisations
Provider Organisations have both a statutory and contractual duty to have systems in place for robust and timely management of SIs (see NHS England Serious Incident Framework, March 2015), including identification, investigation and implementation of actions for improvement. This includes working with other organisations to investigate cross-boundary SIs. Provider organisations are held to account for their management of SI's as set out in this guidance.

Each Provider Organisation must have a local policy that includes SI management in line with this procedure and covers internal responsibilities for SIs, formal Si investigation approach, assurance and reporting to their Organistion's board, to the CCG and any other relevant agencies.

The Provider Organisation must ensure that all their Commissioners are aware that a Serious Incident has occurred and that, all Serious Incident reports, including trend and theme analysis, are similarly made available to each Commissioner. This includes NHS Foundation Trusts, the Independent Sector, and Care Homes where the CCG is paying for the care provided.
The provider Organisation is also required to ensure that response to assurance requests following serious incident investigation reviews are provided within the specified 28 day timescale.

The **Chief Executive** of the Provider Organisation is required to identify an Executive Lead for the management of incidents. The Executive Lead will be required to implement an effective risk management system, providing staff with a clear framework for prompt incident reporting, including training and support ensuring that appropriate actions are taking place, that risk is mitigated and there is a strong culture of learning and improvement.

If more than one Provider within the locality is involved in a SI, the organisation that has identified the incident will inform the commissioning CCG (via the Federated Clinical Risk management team). The Provider Organisations will decide on who the coordinating organisation will be and notify the Federated Clinical Risk Management team. The co-ordinating organisation will, in discussion with the aforementioned organisations, arrange a meeting that includes all key stakeholders to establish the scope of the investigation and terms of reference. At this meeting a lead professional of an appropriate level and seniority will be nominated to lead

the investigation. All key stakeholders will work with the nominated lead to ensure a comprehensive report is produced.

All Provider Organisations will ensure they have a mechanism in place for regularly reporting all incidents, including SIs to the NHS England Patient Safety Division through the National Reporting and Learning System.

Provider Organisations are responsible for the completion of all relevant sections on STEIS and for updating the account with the outcome of the RCA investigation.

To enable the CCG Commissioners to monitor the risk profile of the Provider, Providers are required to provide high level detail of **all SI's** reported by their Organisation (regardless of whether a commissioned patient or not).

Provider Organisations must inform the commissioner if they are considering commissioning services (or parts thereof) through other Organisations. In this situation the Commissioner will require assurance that the Contract / Service level agreement in place, ensures Patients Safety is incorporated in line with this policy.

If more than one NHS organisation is involved in a Serious Incident (SI)
A SI may cover several stages of a patient's pathway, with different Organisations involved in providing care. Many SIs arise from people who fall between gaps in services. To gain the most from a SI investigation, all relevant Provider Organisations should work together to review care within and across boundaries. If the reporting organisation is unable to secure involvement from all parties involved in providing patient care (within the episode of care subject to investigation), support to secure appropriate level of engagement can be secured from the Federated Clinical Risk Management Team.

The Federated Clinical Risk Management Team would liaise with the relevant Provider Organisations to secure engagement. The responsibility for the lead of the RCA process would sit with the Provider Organisation who is best placed to assume responsibility for coordinating the incident. Where there is no Provider Organisation in a position to assume responsibility, the process may be led by the Federated Clinical Risk Management Team on behalf of the CCG.

Where a serious incident notified includes primary care involvement, the CCG should be notified immediately. The CCG will be responsible for co-ordinating the serious incident investigations for those incidents where the primary care element constitutes the largest proportion of investigation required (see appendix 1).

At all stages of a SI investigation, the reporting Provider Organisation must consider if any other Organisations should be involved, and should make contact at the earliest opportunity. To support the management of the SI investigation where more than one organisation is involved, the Provider organisations must agree (as referenced above):

- The lead organisation coordinating the SI process
- The lead contacts for each organisation
- Who will be the one point of contact with the patient, carer or family?
- (Where the SI was received as a complaint, the Provider Organisation receiving the complaint will have already made contact with the complainant and it would be best if this relationship was maintained.)
- A timescale for completion of individual investigations
- A meeting to review cross-boundary issues
- Agreement on who will submit updates and the final report and action plan to the CCG
- Agreement on how cross-boundary recommendations will be taken forward
- If a SI involves three or more organisations, the Provider Organisations involved may feel that it would be helpful for the CCG to co-ordinate the SI process. In this case the lead Provider Organisation should

contact the CCG to determine if this is appropriate. If the CCG agrees to co-ordinate the SI, it will carry out the following functions:

- Agree who will be the main point of contact with the patient, carer or family (there should be one nominated person liaising with the family, with agreed back-up in case of sickness).
- Collate and circulate the names of the leads from each organisation
- Organise an initial multi-organisation meeting chaired by the Director of Quality; Nurse member, or a deputy to agree terms of reference for the investigation and a timetable for the SI process.
- Receive and circulate the reports and action plans from the individual Organisations.
  Where necessary, arrange and facilitate another multi-organisation meeting to review individual reports, discuss cross boundary issues, and agree cross boundary recommendations. Agree who will complete the final cross-boundary report and action plan.

If the Police or Health and Safety Executive (HSE) are involved in an SI, the principles outlined in the memorandum of understanding between the police, HSE and Department of Health should be followed. If the police are involved, the parameters of the local investigation will be guided by them in the first instance. If any restrictions are placed on Organisation investigators by either the Police or HSE these should be clearly documented in the Organisation records, in associated reports to the Organisation and reflected on STEIS.

SIs Identified in a Different Organisation
The NHS England Serious Incident Framework, March 2015 require all incidents that occur in NHS-funded services or while providing NHS-funded care to be reported. Therefore any member of staff who identifies a SI while carrying out their role has responsibility to ensure the SI is reported, irrespective of where the care occurs. Ideally this will be done by the Organisation where the care occurs, once the concern has been raised. Organisations should work together to ensure there is learning from all SIs.

If the Organisation where the care occurred is unwilling to report the SI, the identifying Organisation must report the SI and provide details of the investigation that has brought the incident to light. The CCG understands the concern that Organisations may have in reporting a SI in circumstances when they are not able to directly carry out any recommendations. In this case, the CCG will record the SI under the CCG, where the care has been commissioned by the CCG. In this situation, the reporting Organisation has a duty to discuss with the other Organisation providing the care and to carry out the investigation of the incident as far as possible.

SIs in subcontracted or commissioned services
Some Provider Organisations sub-contract part of their services to other organisations. Similarly, some commission services from other Provider Organisations.

If an SI occurs in the sub-contracted or commissioned services, the Provider organisation retains responsibility for the management of the SI. They are required to report the SI, and to monitor the management and investigation of the SI in the sub-contracted or commissioned service.

In some cases, Provider Organisations may have delegated responsibility from a Commissioner for managing and monitoring all or part of a service in another organisation. In such cases, the Provider Organisation will again manage and monitor the investigation and action plan implementation of the SI.

Approach when managing serious incidents relating to non-Lincolnshire residents:
Some Provider Organisations have multiple Commissioners (commissioners including other CCG's, Specialised Commissioning and NHS England). In these circumstances, principles for identifying who will do what for the purposes of serious incident management are key. In principle, the Organisation responsible for receiving and closing the SI will be the lead commissioning organisation.

Given however that there is currently significant variability in the way that Commissioners approach this, should the situation arise, that a Provider reports on STEIS an SI relating to care commissioned by another CCG / Organisation, the Federated Clinical Risk Management Team will liaise with the other Commissioner to clarify on a case by case basis who will lead the management and close the SI.

Requirements for reporting SIs to other agencies

NHS England

NHS England has a direct commissioning role as well as a role in leading and enabling the commissioning system. NHS England is responsible for reviewing trends, analysing quality and identifying issues of concern. In addition, NHS England may also be required to lead local, regional and national responses to homicides, where the patient is in receipt of mental health services. Therefore incidents relating to services directly commissioned by NHS England should be notified on initial received of the incident detail.

Care Quality Commission

The CQC makes authorative judgements on the quality of health and care services according to whether they are safe, effective, caring, responsive and well-led. The CQC works closely with commissioners and providers to gather intelligence and information as part of their pre-inspection process. The Health and Social Care Act sets specific requirements for registered organisations (Providers) in relation to the type of incidents that must be reported to them. Providers have a responsibility to report to the CQC serious incidents that relate to patient safety/patient harm.

Monitor

Monitor utilise information and intelligence from Commissioners to inform their monitoring of existing NHS Foundation Trusts, and the authorization process for new NHS Foundation Trusts. Monitor and utilise information on serious incident reports, investigations and action plans to monitor Foundation Trust's compliance with essential standards of quality and safety and their license terms.

NHS Trust Development Authority (TDA)

The TDA support NHS Trusts to ensure that they have effective systems and processes in place to report, investigation and respond to serious incidents in line with national policy and best practice. The TDA work in partnership with Commissioners responsible for holding Trusts to account for their responses to serious incidents.

National Learning and Reporting System

All incidents must be reported via the Provider organisation risk management system to the NHS England National Reporting and Learning System (NRLS), who will report to the Care Quality Commission (CQC). This ensures the organisation meets the CQC registration requirement 18 (and part of 20).

Although some notifications are made to the CQC via the NRLS, the CQC stress that their notification requirements are as set out in the Health and Social Care Act 2008 regulations (referenced above) and the Essential Standards guidance, not as set out in the NHS England Incident Reporting framework. The CQC notification requirements for Outcome 20 extend beyond SI reporting and include notification of 'any abuse or allegation of abuse in relation to a service user'.

Similarly, for notification of the death of a service user, the CQC require Provider Organisations to use the definition from their regulations; they do not refer to the NHS England Incident Reporting framework.

All Safeguarding SIs should be reported to the relevant safeguarding leads, as detailed further on within this policy.

Immediate action to be taken following an SI

A safe environment should be re-established as soon as possible. The risk of recurrence should be considered immediately and actions taken to mitigate in advance of the investigation. Any urgent clinical care that may

reduce the harmful impact of the incident must be given immediately.

The needs of patients and their family/ carers are a priority and they must be kept informed reflecting the contractual requirement of 'duty of candour'. The need for reporting to the local Safeguarding Board should also be considered at this point.

All relevant equipment or medication should be quarantined, labelled and isolated as appropriate. To maintain product liability, no piece of equipment should be returned to the manufacturer for repair /examination until the provider has carried out all necessary tests on the equipment as suggested by the MHRA.

A contemporaneous and objective entry should be made in the patient's clinical records and, where necessary, statements taken using a supportive statement taking process.

Relevant documentation should be copied and secured to preserve evidence and facilitate investigation and learning.

The organisation's communications team should be notified of the incident and a relevant communications policy for dealing with serious incidents triggered where appropriate

Process for reporting and updating CCG's regarding SI's
Initial reporting
All commissioned Provider organisations are required to report all SIs on STEIS (Strategic Executive Information System) without delay and within two working days of the incident being reported/ becoming known.

Incidents that activate the NHS Trust or Commissioner Major Incident Plan; are of significant patient concern; give rise to significant media interest or will be of significance to other agencies such as the police or other external agencies should be reported immediately to the relevant commissioning organisation via telephone as well as electronically.

If the incident is identified outside of normal working hours the On Call Director should be contacted. Internally, the CCG Communications lead will be made aware if media interest is likely. Subsequent SI reports should record an update on any media queries and statements issued.

On receipt of the serious incident notification, consideration should be given to other regulatory, statutory, advisory and professional bodies that should be informed, inclusive of but not limited to the CQC; Controlled Drugs Accountable Officer; Coroner; Defects and Failures; Health and Safety Executive; Health Education England; Information Commissioners Office; Local Authorities; Medicines and Healthcare Products Regulatory Agency (MHRA); Monitor; NHS Trust Development Authority; Police; and Public Health England.
If an organisation does not have access to STEIS, the provider should notify the Federated Clinical Risk Management Team by telephone and send details of the incident to the CCG SI inbox. The incident will be assessed upon receipt by the clinical risk management team, escalated to the CCG Executive Lead Nurse for Quality and Patient Safety as necessary and uploaded onto STEIS.

An automated email will be sent to the CCG / Area Team notifying them that an incident has been reported. Some incidents do not come to light as soon as they occur. If the incident is not identified immediately as a serious incident, details of the reason for the delay will be required when submitting the SI form. The CCG will determine if the reason given is acceptable. Provider constraints with capacity and capability are not considered valid and acceptable reasons for delay in reporting SIs.

Determining the Level/Type of Investigation
The level of response to a serious incident will be dependent upon the nature, severity and complexity of the incident that has occurred. It is important that the level of investigation is proportionate to the circumstances of the incident and determined by the Provider Organisation as part of the preliminary review process.

The Provider will be responsible for advising the Commissioner of the level of investigation that will be undertaken. Whilst the level of investigation is established as part of the preliminary review of the incident, this may be subject to change as new information or evidence emerges as part of the investigation process.

There are three levels of investigation identified within the NHS, as follows:
- Level 1 – Concise Internal Investigation
- Level 2 – Comprehensive Internal Investigation
- Level 3 – Independent Investigation

Further detail on the three investigation levels are detailed within Appendix 2

If after initial investigation, the Provider organisation feels that it does not meet the criteria for an SI then an update should be submitted to the CCG stating the reason and request a retraction. If the CCG feels that this is appropriate, the SI will be downgraded on STEIS and closed**.**

Preliminary Reports
An initial review should be undertaken within 72 hours and preliminary report should be sent to the CCG and uploaded onto the STEIS system within 3 working days for all SIs (see Appendix 3). Other updates may be requested by the CCG and should be submitted within the requested timeframe**.** This will provide more detail to assure the CCG that immediate actions have been taken and that the investigation has commenced.

The aim of the initial review is to identify and provide assurance that any necessary immediate action to ensure the safety of patients, staff and the public is in place; to assess the incident in more detail (establishing that the incident meets the criteria for serious incident reporting) and to confirm the level of investigation required.

Where, on notification of an incident, there is concern that there may be more significant implications for the wider healthcare system, the CCG will consider the need to escalate and share information with NHS England and other partner agencies as required.

Reporting SIs that occur outside normal working hours
In most cases, SIs that occur outside normal working hours can be reported to the CCG at the start of the next working day or notified via the SI telephone: Tel Number: 01522 515415.

Out of hours, if the Provider is concerned that the incident should be reported immediately, they should contact the on Director on call.

Examples of incidents that may require immediate reporting include:
- Never Events
- Fire in NHS premises
- Infectious disease outbreak
- Major Incident plan invoked such as major failure of IT or communications systems
- Incidents that result in adverse media coverage or public concern about the quality of healthcare or an organisation

Serious Incident Investigation Report Requirements
The serious incident investigation report and associated action plan should be submitted to the Commissioner within 60 working days of the incident being reported. An extension to the 60 working day deadline can be approved by the Commissioning Organisation, where the Provider has identified sufficient reason for the deadline not being achievable i.e. complexity of the incident; investigation of highly specialised and multi-organisational incidents etc.

Requests for extensions to the serious incident investigation report deadline must be submitted in writing, in advance of the original deadline (Appendix 4)

In circumstances where an extension to the investigation timeframe has been agreed, the revised deadline should be recorded within the serious incident management system and included in the serious incident report.

Where the serious incident is subject to an independent investigation, a deadline can be agreed with the Commissioner for 6 months from the date the investigation commenced.

The final report should follow the NHS England (RCA investigation report template and include details of the RCA, lessons learnt, details of dissemination of learning, and an action plan with recommendations, timescales and responsibilities for action. Actions should be SMART (specific, measurable, achievable, relevant and have a realistic timescale). The report should show reflection on the root causes and consideration of what needs to change following the SI.

Details of the headings to use in the final report are available on the NPSA website at:
http://www.nrls.npsa.uk/resources/root-cause-analysis

The investigation report submitted should include a SMART action plan. In line the NHS England Serious Incident Framework, it is recommended that the NPSA Action Plan template is utilised:
http://www.nrls.npsa.nhs.uk/resources/collections/root-cause-analysis

All incident investigation reports should have been reviewed and signed off at a senior executive level within the provider organisation before submission. Details of who signed off the investigation report must be reflected on the investigation front sheet.

The clustering of incident investigations is subject to discussion between the commissioner and provider, and should be undertaken in accordance with the agreed national guidance.

Review of investigation credibility and thoroughness of final reports
On receipt of the investigation report from the provider organisation, an initial review will be undertaken by the Federated Clinical Risk Management Team; to establish that the report meets to minimum investigation report criteria as defined by the NPSA (Appendix 5). Where an investigation report does not meet the minimum requirements, the document will be returned to the Provider Organisation, along with the review undertaken by the Federated Clinical Risk Management Team.

The Provider Organisation will have 28 days within which to resubmit the serious incident investigation report.

Those serious incident investigation reports that meet the minimum investigation requirements will be submitted to the monthly serious incident review group. Within the serious incident review group CCG Executive Nurses will review the final report to determine if all aspects of the incident have been adequately investigated.

Where necessary, further specialist advice will be sought as part of the serous incident investigation report review process i.e. safeguarding, mental health, specialist secondary care colleagues. Membership will be co-opted onto the serious incident review group as required.

Assurance may be sought from Provider Organisations following the serious incident investigation review undertaken. Provider Organisations will be expected to provide a response to assurance requests within 28 working days.

Monitoring of SI management and escalation of concerns
The CCG monitors Provider Organisations' management of SIs and will ask for further investigation or action at any stage in the process if required, including additional actions following SI investigation such as clinical audit and cross-boundary collaboration. Thematic reviews are carried out when indicated. The CCG considers learning from all SIs, reviews trends and manages dissemination of learning across the health economy where appropriate.

The CCG will produce a quarterly compliance report for each Provider Organisation which is sent to the CCG Contract team and Provider Organisations a week prior to the Contract Quality Review (CQR) meeting.

If there are any queries about the assessment of a final report or timeliness data, the initial appeal process would be to the Federated Clinical Risk Management Team, who will confer as necessary with the appropriate Executive Nurse(s), to respond.

Concerns regarding SI performance will be escalated as necessary to the relevant CCG Quality and Patient Experience Committee and the Contract Quality Review meetings, potentially leading to generation of a Contract Query and need for a Remedial Action Plan as outlined in the Contract Schedule.

Action if timescales for submission of final report are not likely to be met
If it is likely that the investigation and production of the final report will not be completed within the required timescales, the progress of the investigation and the reasons for the delay must be outlined and reported to the CCG as soon as known. The CCG will then consider whether a temporary exception date for submission would be appropriate and document and update the STEIS form accordingly. As referenced earlier in the policy, problems with capacity and capability will not generally be accepted as a valid reason as the Provider needs to ensure they are able to meet their contractual responsibilities with regards to SI investigation and reporting.

Stop the Clock
As referenced within the NHS England Serious Incident Framework (March 2015) the undertaking of a criminal investigation is not an automatic bar on the completion of a serious incident investigation. Wherever possible, serious incident investigations should continue alongside criminal proceedings. This should be considered in discussion with the police.

Following a formal request by the police, a coroner or a judge, the investigation may be put on hold, as it may potentially prejudice a criminal investigation and subsequent proceedings (if any). Where this is the case, the Provider Organisation should complete the necessary stop the clock request form (Appendix 6), complete with a copy of the formal request received. The Executive Lead Nurse for Quality and Patient Safety will then review the request and agree a date for completion once the investigation can recommence.

Penalties for late submission
Penalties will be attributed for the late submission of serious incident investigation reports to the Federated Clinical Risk Management Team as outlined in the Contract agreement.

Closure of SIs and Action plan monitoring
The final report and action plan will be reviewed by the CCG and any queries clarified. Once the CCG feels assured that the SI investigation has been thorough and appropriate and the process followed, the Federated Clinical Risk Management team will on behalf of the CCG Executive Lead Nurse for Quality and Patient Safety, close the incident on STEIS.

In some instances the SI will be closed on STEIS whilst still awaiting evidence of action taken. In these circumstances, this decision will be risk assessed and the action / outstanding assurance held on CCG serious incident system within Datix until sufficient assurance is received.

Progress on implementation of these action plans will be monitored via the SI Review Group and Patient Safety meetings. Enduring concerns will be reported to the CCG Quality and Experience Committee and to the relevant Provider Quality Review Meeting and reported within the Patient Safety report.

An SI may be closed even though an inquest is to be held, however if the Inquest outlines recommendations for the Provider, the Provider should inform the CCG and the SI may be reopened. The SI action plan should be updated if required following the Inquest findings, and re-submitted to the CCG.

Summary of learning for dissemination
Learning following an incident is essential to improve practice and prevent similar incidents occurring again. Examples of learning are given below:

- Solutions to address SI root causes that may be relevant to other teams, services and Provider organisations. Identification of the components of best practice that reduced the potential impact of the SI and how they were developed and supported.
- Lessons from conducting the investigation that may improve the management of investigations in the future
- Documentation of the identification of the risks, the extent to which they have been reduced and how this is measured and monitored
- Identification of any relevant staffing issues e.g. skill mix, recruitment, induction and training that may prevent further incidents
- Identification of not meeting relevant CQC essential standards
- Identification of any safeguarding lapse

To increase the impact of the improvements in care resulting from SI investigations, the CCG will support dissemination of key learning across the health economy where appropriate.

As part of the final SI report, Provider Organisations should provide a short summary that they can share with other organisations. This can be the Executive Summary already included in the report if this is appropriate. It must include learning from the SI and any good practice identified. The Provider organisation can disseminate this summary through its own network, or ask the CCG to disseminate as appropriate. When using the former route, the final report should give details of the dissemination plan.

Never Events
Never Events are serious, largely preventable patient safety incidents that should not occur if the available preventative measures have been implemented. The Department of Health (DH) produces a list of Never Events which is updated annually.

The Never events Framework -2015/16 (updated March 2015) provides the list of never events

Never Events Listings

1	Wrong site surgery
2	Wrong implant/prosthesis
3	Retained foreign object post-procedure
4	Mis-selection of a strong potassium containing solution
5	Wrong route administration of medication
6	Overdose of insulin due to abbreviations or incorrect device
7	Overdose of methotrexate for non-cancer treatment
8	Mis-selection of high strength midazolam during conscious sedation
9	Failure to install functional collapsible shower or curtain rails
10	Falls from poorly restricted windows
11	Chest or neck entrapment in bedrails
12	Transfusion or transplantation of **ABO**-incompatible blood components or organs
13	Misplaced naso or oro-gastric tubes
14	Scalding of patients

When a Never Event is reported, Provider Organisations are required to provide the following specific (anonymised) information for each member of staff involved:

When was their last appraisal?

Did the appraisal include (relevant to the issue) adherence to the WHO Surgical Checklist
Whether this is the first issue with which the individual has been involved
What remedial or disciplinary action has/ is being considered or has been taken to that point
If referral to a professional body - GMC, NMC, HPC has occurred status of that referral to date.

This information should form part of the preliminary report (72 hour early management report) and this should be submitted to the Federated Clinical Risk Management Team. The final investigation report must also include a full update on this issue. A copy of the 72 report should use the Incident Decision Tree when assessing whether management action is appropriate for an individual available via http://www.nrls.npsa.nhs.uk/resources/?EntryId45=59900

Never Events must attract in-depth management and review and as such will always be reported as grade 2 SI. The Federated Clinical Risk management Team will require a preliminary report within 72 hours and further updates of the progress with the investigation if requested.

A Never event summit will be convened following receipt of the Never Event RCA. This will comprise of a meeting between senior Provider and ULHT representatives, with the purpose of evaluating the level of investigation undertaken, actions agreed. Specific attendance of speciality ward leaders at this meeting and prior site visit to the clinical area will provide opportunity to assess how embedded required actions are, before closure on STEIS is agreed.

Seeking Recovery of Cost if a Never Event Occurs
Whilst cost recovery is secondary to the process of reporting never events, learning from them via robust investigation and implementation of learning to prevent any future reoccurrence; NHS Organisations should not pay for care that is so substandard as to result in a never event. For this reason CCGs should seek to withhold payment for the cost of the episode of care in which a never event has occurred and any subsequent costs involved in treating the consequences of a never event. As specified in The Never Events Policy Framework, March 2015.

In addition to recover of the cost of the procedure/treatment. CCGs will seek from the provider a remedial action plan to ensure that future breaches are avoided. The management of this plan will be through the monthly contract review process, and any breach may results in contract withholding in accordance with contract performance mechanisms set out in the NHS Standard Contracts.

SIs relating to safeguarding children
The CCG requirements for reporting a serious incident relating to children and young people is informed by the NPSA Information Resource, Working Together to Safeguard Children (2015) and Policies and Procedures from Safeguarding Children Boards.

Where an incident involves a child or young person, it is the responsibility of all employees to inform their direct line manager and to be compliant with the organisations policies and procedures.

When a safeguarding incident is also subject to investigation with the Local Safeguarding Children Board or organisational independent management review, the process will inform and provide reports as required within the SI process. It will not be required to complete a separate investigation.

For unexpected child deaths the Child Death Overview Panel may recommend to the CCG that a child death should be reported and investigated as an SI. The Designated Pediatrician with responsibility for unexpected deaths may, in discussion with the CCG safeguarding team, also recommend an SI on reviewing the information gathered through the unexpected child death protocol.

The Designated Nurse for Safeguarding Children will be included in the distribution of any SI's involving children.

It is recommended that where there is any uncertainty regarding the reporting or notifying of a Serious Incident to the CCG, a discussion take place with The Designated Nurse for Safeguarding Children or her Deputy.

It is required to report a Serious Incident in the following situations:-

- A child death where abuse as defined in Working Together to Safeguard Children (2015) is suspected to be a factor in the death (this will investigated through the SCR process).
- Where a child has (or might have) suffered harm as a result of a health care worker omitting to follow procedures or staff fail to act where there are clear suspicions of abuse (such as patterns of neglect, high risk indicators of persistent abuse).

SIs relating to safeguarding adults
There is a clear and set process for investigating and taking action in relation to an Adult Safeguarding (AS) investigation. There is also a clear and set process for investigating a Serious Incident (SI) as defined by NHS England Serious Incident Reporting Framework 2015.

An AS incident must also be reported as a SI if it meets the NHS England definition in relation to the abuse of an adult as described in "No Secrets," as follows:

- There is death or injury to a vulnerable adult where abuse or neglect is suspected to be a factor.
- A vulnerable adult has suffered harm as a result of staff failing to follow agreed procedures or acceptable practice.
- A vulnerable adult has suffered significant injuries suspected to be as a result of abuse
  There are systemic problems relating to care of vulnerable adults

If a SI is being investigated under the AS process, the AS investigation will provide the necessary documentation and reporting requirements for the SI, so no duplication is necessary. The process below builds on the Local Authority Adult Safeguarding documentation to give the requirements and responsibilities for SI reporting.

The table below outlines the responsibility of the Provider in reporting SIs relating to Adult Safeguarding.

Stage	Function	Responsibility	Time Frame
Initial referral	Record information and report to manager, record allegations and concerns of abuse or neglect, deal with immediate protection	Everyone responsible for initial response	Immediately on the same day
Referral details sent to team	Refer allegation to the local team and Adult Safeguarding Lead	Duty, locality team, Adult Safeguarding Lead, Emergency Duty Team	Within 24 hours, including out of hours
Strategy Discussion	Decide if safeguarding procedures are appropriate, and level of response. If not, identify alternative responses. If yes, discuss with Police whether a crime has been committed - if yes, refer to Police. Decide if incident meets the definition of a SI. If so, report to commissioning organisation using SI form.	Adult Safeguarding Lead, in consultation with other organisations Line Manager Adult Safeguarding Lead	Within 24 hours
Strategy discussion and/ or professionals meetings	Formulate a multi-agency plan for assessing risk and addressing any intermediate protection needs. Provide update to SI lead in commissioning organization	Adult Safeguarding Lead, with other organisations	Within 5 working days
Investigation, assessments, professionals meetings and strategy meeting as	Co-ordinate the collection of information about concerns - abuse or neglect that has, or may, occur. This may include an	Adult Safeguarding Lead and other organisations	As decided through the strategy discussion, but within 4 weeks from the

Stage	Function	Responsibility	Time Frame
required	investigation, criminal, and/or disciplinary investigation. Provide update to SI lead in commissioning organisation. If the case meets the criteria for a Serious Case Review (SCR) then a referral should be made to the SCR Sub Group as per the Safeguarding Adults Multi-Agency Policy and Procedures		alert
Safeguarding action plan – development, implementation and review.	Analyse concerns, investigation and decisions made in discussions and meetings. Develop Adult Safeguarding Action Plan at strategy meeting. Allocate actions to appropriate organisations. Identify time scales to monitor and review actions. Refer to MARAC if appropriate.	Safeguarding partner organisations as appropriate	As identified from discussions, professionals meetings, strategy meeting
Serious Incident process (SI)	Provide final Adult Safeguarding documentation to SI lead in commissioning organization. If Adult Safeguarding documentation does not meet the SI requirements, SI lead to discuss any further information required with Adult Safeguarding lead	Adult Safeguarding lead SI lead	Within 9 weeks of incident date. If this timescale cannot be met, discuss with SI lead and agree appropriate extension. Repeat as necessary Within 2 days of receiving documentation
Review	Review the Adult Safeguarding Action Plan Provide update to SI lead in commissioning organisation	Adult Safeguarding Lead, with other organisations as relevant	First review as identified in the Adult Safeguarding Action Plan
Recording, monitoring and reviewing	Adult safeguarding process Provide update to SI lead in commissioning organisation	Adult Safeguarding Lead	On-going as required.

It is recommended that where there is any uncertainty regarding the reporting or notifying of a Serious Incident to the CCG, a discussion take place with the Lead Nurse for Adult Safeguarding Tel 01476 406599.

For many safeguarding SIs, the investigation will be part of the safeguarding process as outlined above. In those cases, a separate SI investigation report may not be needed, and the safeguarding investigation report will act as a SI report, as long as it includes robust recommendations and action plan.

Some Provider organisations may have responsibility for investigating safeguarding adult concerns for older people over the age of 65 years through a Section 75 agreement. In this situation the Provider organisation would be required to report any safeguarding adult SI identified (in line with the NHS England Serious Incident Reporting Framework 2015), ensure an investigation and final report is submitted, and monitor and report on the implementation of the improvement action plan.

Care Homes
In cases when a care home is involved where an SI is being considered such as CQC concerns, high numbers of grade 3 or 4 pressure ulcers or SOVA referrals, details of residents / patients receiving NHS funded care should be clarified. Information should be shared with the Adult Safeguarding leads at the CCG and Local Authority as outlined above.

SIs relating to Healthcare Associated Infections (HCAIs)
The categories for reporting SIs involving HCAIs are as follows:

Outbreaks of healthcare associated infection (this includes the presumed transmission within a hospital and causes significant morbidity, mortality and or impacts significantly on hospital activity). An outbreak has been defined for the following infections

Clostridium difficile – two or more cases caused by the same strain related in time and place over a defined period that is based on the date of onset of the first case(Department of Health (2008) *C difficile: How to deal with the problem*)
Norovirus- closure of a ward

MRSA bacteremia – all post 48 hours cases
Any death where MRSA bacteremia or C. difficile are recorded on part 1a of the death certificate
Infected healthcare workers (incidents which necessitate consideration of a look back exercise) e.g. HIV, TB
Breakdown of infection control procedures and or serious decontamination failures with actual or potential for cross infection.

The normal SI reporting process should be followed and a full systematic investigation must be undertaken and a full RCA or Outbreak report sent to the CCG, together with an action plan.

SIs relating to Maternal Death
Although not all maternal deaths are classified as SIs, in order to comply with NMC Midwives Rules and Standards 2012 all maternal deaths must be also reported to the Local Supervising Authority Midwifery Officer (LSAMO) via the LSA coordinator.

East Midlands LSA Office, 2nd Floor North, Cardinal Square, 10 Nottingham Road, Derby, DE1 3QT. Tel: 01138 255529.

Personal Data Breaches (Data Security and Protection Incidents)
Personal data is defined as;

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

A Personal Data breach is defined as;

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed."

GDPR places a mandatory requirement on the CCGs to report breaches of personal data. Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner's Office.

Reporting
The incident **must** be recorded on DATIX as soon as possible and within 24 hours of identification, recording all information known at that point. Further detail can be added as necessary. An electronic alert is automatically generated by the DATIX incident reporting system, to notify the Information Governance team of any incidents which include reference to a Data Security and Protection or information governance breach. The Information Governance Team are then able to provide appropriate support to the investigating manager to ensure all necessary action has been taken manage information governance risks identified.

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, Data Security and Protection Incidents could include (i) any incident involving the actual or potential failure to meet the requirements of the Data Protection Act 2018, GDPR and or the Common Law of Confidentiality (ii) unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy (iii) personal data breaches which could lead to identify fraud or have significant impact on individuals. The examples above, apply irrespective of the media involved and includes both electronic media and paper records relating to staff and service users.

The clinical risk management team and the Information Governance Lead will informally advise the relevant CCG's Chief Operating Officer, Senior Information Risk Owner, Data Protection Officer and Caldicott Guardian.

If the incident scores anything other than 'grey' in the breach assessment below, the DHSC & ICO must also be notified. The incident should be recorded on the Data Security and Protection Toolkit Incident Reporting Tool, and the DHSC and ICO will be automatically notified once submitted.

Grading the personal data breach (Assessing the severity)

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. Incidents should be reviewed by the Data Protection Officer, Caldicott Guardian or Senior Information Risk Owner when determining what the significance and likelihood of a data breach will be.

Establish the likelihood that adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach

Grade the potential severity of the adverse effect on individuals

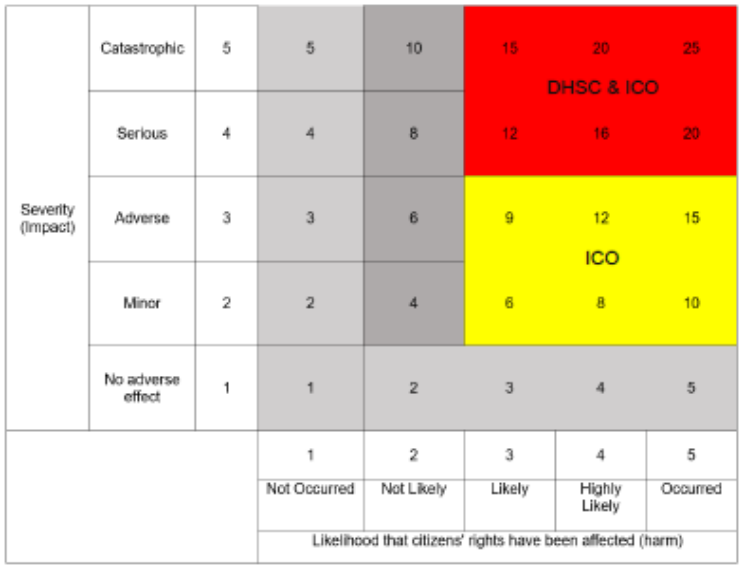
No.	Likelihood	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event	A person dies or suffers a catastrophic occurrence

There are a limited number of circumstances where, even when the CCGs are aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances notification may not be necessary:

- Encryption – where the personal data is protected by means of encryption
- 'Trusted' partner – where the personal data is recovered from a trusted partner
- Cancel the effect of a breach – where the Data Controller can null the effect of any personal data breach

Breach Assessment Grid
This operates a 5 x 5 basis with anything other than 'grey' breaches being reportable. Incidents where the grading results are in the red should be notified within 24 hours.



Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, full details will be automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

The Department for Health and Social Care will also be notified where it is (at least) likely that harm has occurred and the impact is at least serious.

Content to be included in Annual Reports
High risk incidents, those of which are reportable to the Department of Health and Social Care and the Information Commissioner's Office need to be detailed individually in the annual report in the format provided. All reported incidents relating to the period in question should be reported, whether they are open or closed incidents.

Annual Governance Statement (AGS)
The AGS 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 the organisation and by reference to the organisations use of the Data Security and Protection Toolkit.

Any incidence of a reportable Data Security and Protection Incident should be reported in the AGS as a significant control issue. For the avoidance of doubt, refer to the breach assessment grid above (those with an assessment score which falls into the red or yellow categories).

SIs relating to Pressure Ulcers
All Grade 3 and 4 pressure ulcers are reportable where they meet the serious incident criteria.

If the Grade 3 or 4 pressure ulcer developed 72 hours or more after the decision to admit or admission to caseload / service then it is deemed as being acquired within the present provider organisation. The Provider organisation should report this as an SI via STEIS and investigate the pressure ulcer themselves.

If the pressure ulcer is present on admission or develops in less than 72 hours from the decision to admit or admission to the caseload / service, the current Provider organisation should notify the Provider organisation where the pressure ulcer was thought to have developed for them to report as an SI and investigate

Pressure Ulcer SI investigations are subject to the normal 60 day timescale for submission of the final report. It has been agreed that the Director of Nursing in the Provider organisation has a process for reviewing pressure ulcer investigations and sign them off before they are submitted to the CCG for review. Submitted RCAs will be subject to the same RCA review processes as other non PU RCAs, namely reviewed by the SI group prior to closure.

Whenever a patient has a grade 3 or 4 pressure ulcer there must be consideration as to whether there is a safeguarding concern. The decision must be documented. If a concern is identified local procedures should be followed.

Definition of an avoidable pressure ulcer
"Avoidable" means that the person receiving care developed a pressure ulcer and the Provider of care did not do one of the following: evaluate the person's clinical condition and pressure ulcer risk factors; plan and implement interventions that are consistent with the persons needs and goals, and recognised standards of practice; monitor and evaluate the impact of the interventions; or revise the interventions as appropriate."
Source: DH Nurse Sensitive Outcome Indicator No 1 - No Avoidable Pressure Ulcers

Immunisation Incidents in Primary Care
The national immunisation programmes are commissioned by NHS England and specifically by the public health commissioning team within NHS Central Midlands. These immunisation programs are not included in the co-commissioning arrangements for primary care currently.

Incidents and serious incidents that are reported by general practice involving immunisations should be notified to the public Health team via telephone or generic email address england.llimms@nhs.net

Professional Misconduct
The majority of serious incidents are caused by the failure of systems/processes and not the actions of an individual. If grounds for professional misconduct are suggested, it is important that the appropriate lead within the organisation (Provider/CCG) is alerted to ensure that appropriate action is taken. Appropriate action includes investigation and/or HR team taking time to carefully assess or refer on to experts the actions or omissions in question within the context of the incident. The incident decision tree should be used to determine if action is required in relation to individuals.

Radiology
Severe equipment failure leading to harm or death.

Screening Programmes
National screening programmes are public health interventions, which aim to identify disease or conditions in defined populations in order to either reduce morbidity or mortality. Screening programmes are sometimes made complicated because the activity of screening often takes place within pathways across several

organisations.

Often there are a wider range of organisations involved including those at a national level and organisations who externally quality assure the screening programmes.

Serious incidents in NHS National Screening Programmes must be managed in line with the guidance 'Managing Safety Incidents in National Screening Programmes as defined within the NHS England Serious Incident Framework 2015.

The management of these incidents is often complex, requiring robust co-ordination and oversight by the Screening and Immunisation teams working within Sub Regions and specialist input from Public Health England's Screening Quality Assurance Service.

The Screening Quality Assurance Service is also responsible for surveillance and trend analysis of all screening incidents. It will ensure that the lessons learnt are collated nationally and disseminated.

The screening programmes which are covered are:

- Breast cancer
- Cervical screening
- Bowel cancer
- Diabetic retinopathy
- Abdominal aortic aneurysm
- Fetal anomaly
- Infectious diseases in pregnancy
- Sickle cell and thalassemia
- Newborn blood spot
- Newborn hearing
- Newborn and Infant Physical Examination

Staff-Related Incidents
Serious complaints about a member of staff or primary care contractor or any incident relating to a staff member where adverse media interest could occur.

Any serious criminal acts involving patients or staff.

Suspicion of a serious error or errors by a member of staff, primary care contractor or other healthcare contractor.

Where a member of staff is suspected of harming patients.

A serious drug error, such as mal-administered spinal injections.

Where professional competence is in question.

A serious breach of confidentiality.

Where a member of staff is suspected of committing serious fraud.

The exclusion of employed doctors or dentists under the NHS Trust disciplinary procedures that refer to 'High Processional Standards in the Modern NHS: a framework for the initial handling or concerns about doctors and dentists in the NHS' (HSC 2003/12).

Significant disciplinary matters of other staff.

Serious verbal and/or physical aggression.

Where a member of staff shows gross disrespect for the dignity of a patient/deceased patient.

SIs which include HR Investigations
Some SIs will include HR concerns about Provider staff. The NPSA Incident decision tree should be used as a guide. Whilst the detail of HR proceedings are confidential, the Provider investigation must look at the systems in place to support the work of staff relating to the SI, and whether more robust systems could have prevented the incident.

The SI final report should cover this system review, and should state that all HR procedures have been followed as appropriate and that actions agreed from this process are in place and are being monitored. Brief details of the type of action e.g. reflection, case review, training, disciplinary action, referral to professional body should be included in the report. More detailed information should be held in the Provider SI folder for internal audit purposes.

Suicides
Suspected suicide, actual suicide and attempted suicide of any person currently in receipt of NHS services on or off NHS premises must be reported as a SI. This includes:

- Patients currently in receipt of mental health services, or who have been discharged within the last 12 months.
- Patients of primary care practitioners where on review of chronology have identified care/service delivery problems.

Suicide is defined as death where:
- There is obvious evidence or strong suspicion of self-harm, or
- The above does not apply initially but emerges later from a clinical review or investigation of the case, or
- Where the Coroner's verdict is suicide, or where the narrative indicates that the individual took their own life

Terrorism and Chemical, Biological, Radiological or Nuclear (CBRN) Incidents
Any act of terrorism is normally covered under the Major Incident Policy and will therefore have a comprehensive list of definitions. Generally, the following incidents must be reported:

- Terrorist threats/incidents which include incendiary devices or the use of other weapons chemical, biological, radiological or nuclear agents (CBRN)
- Potential or confirmed chemical, biological, radiological or nuclear agents (CBRN) incident.

Violence Towards Health Care Staff
- Counter Fraud and Security Management Service (CFSMS) in the case of fraud and violence to staff. In such circumstances this serious incident framework should be followed in conjunction with national guidance.
- Serious violence/death of healthcare worker.

Complaints
All Provider organisations commissioned by the CCG are required to review learning from all risk information together. This includes information from incidents, complaints and PALS. This requirement is reflected within the Quality Indicators in the contract with the CCG. Thus the management of all risk information should be aligned to ensure learning is maximised from every source.

This management process should also ensure that any complaints or PALS information that meets the definition of a SI is reported as a SI to the CCG.

Management of complaints and SIs has many similarities and reporting a complaint as a SI should not alter the investigation process required. Similarly, most SIs require liaison with the patient, carer or family in a similar way to that carried out as part of the complaints process and as outlined in the Being Open guidance.

However, the outputs required for a complaint and a SI may differ, with the complaint often requiring a very specific response to the questions raised by the complainant, whilst an SI report will focus on the root causes of the incident. It should still be possible to carry out one investigation into the incident, but there may need to be two different responses to satisfy the requirements and timescales of each process.

All staff dealing with complaints must be aware of the CCG procedure for SIs and the CCG's Complaints Policy. It is recognised that it may not be immediately clear whether a complaint meets the definition of a SI. Therefore, part of the initial and on-going complaint review by the Investigating/Service Manager should always include consideration of whether the complaint should be reported as a SI. If there is uncertainty whether the events leading to the complaint meet the SI definition, the compliant should be reported by the Investigating/Service Manager as an SI and revised within 3 working days following discussion and agreement with the CCG, when further information becomes available.

Complaints relating to the following types of incidents must always be reported as SIs:

Avoidable death or serious harm to a patient (If it is unclear if the harm is avoidable, report and SI can be retracted later if required)

Issues relating to safeguarding children or vulnerable adults

Incidents where there is a high probability of media interest

Confidentiality
All SI forms, reports and correspondence should be sent from an NHS net / secure account LIWCCG.ClinicalRiskIncidents@nhs.net

SI forms and reports should not contain any patient or staff identifiable information involved with the incident to comply with Caldecott, data protection and information governance requirements. They should "restrict access to patient information within each organisation by enforcing strict need to know principles".

In any circumstance where it may be necessary to identify an individual, the serious incident lead in the Provider organisation must contact the senior member of the commissioner or local authority to discuss the incident and provide more detailed information.

Information relating to serious incidents (including information held on national systems such as STEIS, local databases and internal reports, investigation reports and root cause analysis and other documents), could be subject to a request for disclosure under the Freedom of Information Act.

Contact details
The contact details relating to SIs are:

Clinical Risk Management Team, LWCCG 01522 515415

Generic in box LIWCCG.ClinicalRiskIncidents@nhs.net

References

Serious Incident Framework, NHS England. March 2015
https://www.england.nhs.uk/wp-content/uploads/2015/04/serious-incidnt-framwrk-upd.pdf

Revised Never Events Policy and Framework. NHS England. March 2015
https://www.england.nhs.uk/wp-content/uploads/2015/04/never-evnts-pol-framwrk-apr.pdf

National Framework for Reporting and Learning from Serious Incidents Requiring Investigation, NPSA March 2010 http://www.nrls.npsa.nhs.uk/resources/?entryid45=75173

Nursing and Midwifery Council Midwives Rules and Standards NMC 2012
https://www.nmc.org.uk/standards/additional-standards/midwives-rules-and-standards/

NPSA Information Resource to support the reporting of serious incidents NPSA August 2010
http://www.npsa.nhs.uk/nrls/reporting/patient-safety-direct

Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation
https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf

DH C difficile infection: How to deal with the problem DH and HPA 2008
http://www.hpa.org.uk/webc/HPAwebFile/HPAweb_C/1232006607827

DH Guidelines for NHS in Support of the Memorandum of Understanding investigation of Safety incidents involving unexpected death or serious harm and a protocol for liaison for effective communications between the NHS, Association of Chief Police officers and Health and Safety Executive gateway 7407 November 2006

NPSA 'Being Open - saying sorry when things go wrong' NPSA Gateway 13015 November 2009
http://www.nrls.npsa.nhs.uk/resources/?EntryId45=83726

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 20, Duty of Candour
http://www.legislation.gov.uk/ukdsi/2014/9780111117613/contents

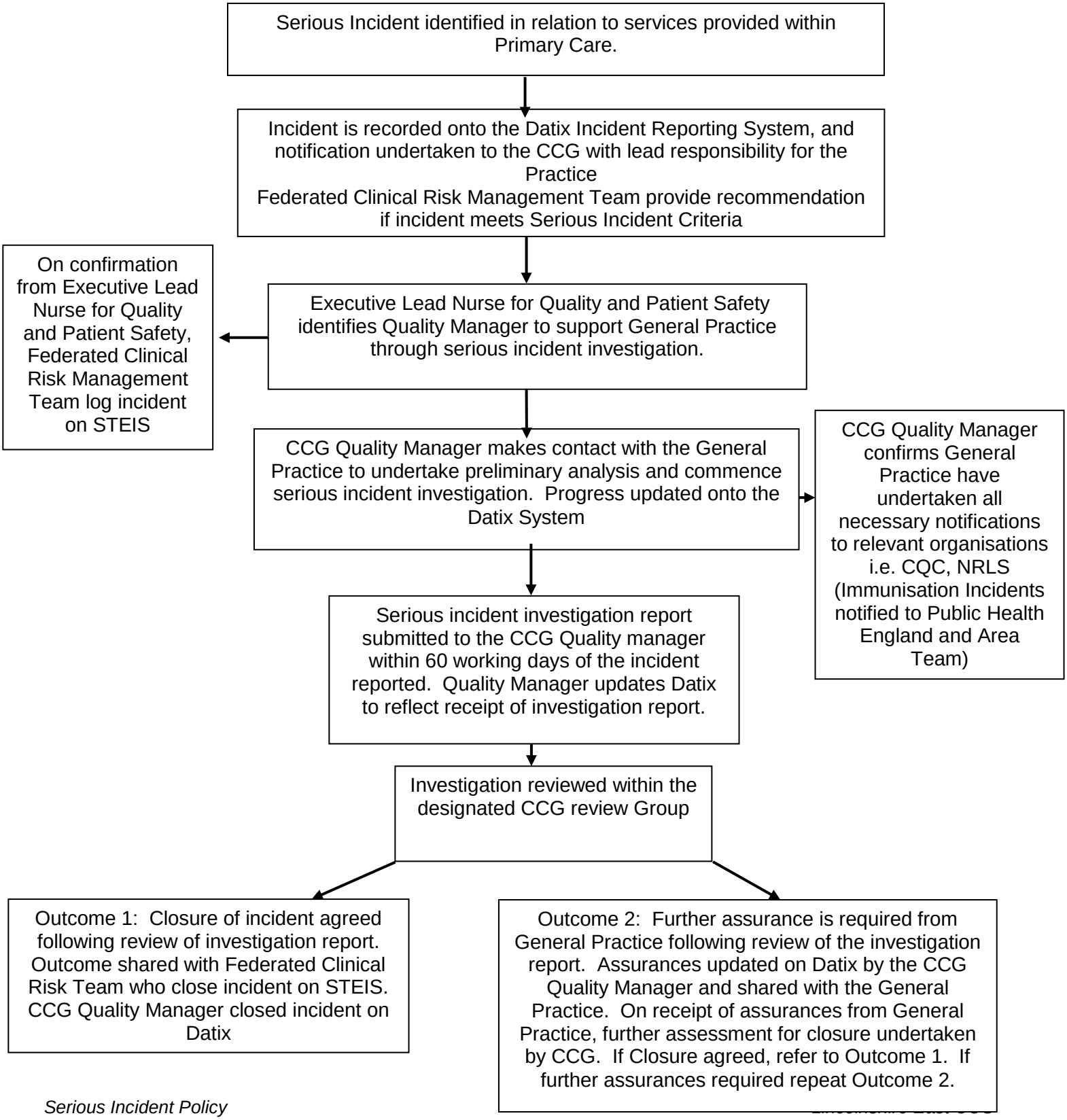
National Quality Board (January 2013). How to establish a Quality Surveillance Group.
http://www.dh.gov.uk/health/2013/01/establish-qsg/

NHS Commissioning Board NHS Standard Contract 2013/14
http://www.commissioningboard.nhs.uk/nhs-standard-contract/

The Care Act 2014
http://www.legislation.gov.uk/ukpga/2014/23/contents/enacted

Care Quality Commission (March 2010). Essential Standards on Quality and Safety.
http://www.cqc.org.uk/organisations-we-regulate/registered-services/guidance-meeting-standards

Primary Care SI Investigation Process



Appendix 2

Level of Serious Incident Investigation

Information in this table provides an outline of the levels of systems-based investigations recognised in the NHS (currently referred to as RCA investigation). Within the NHS, most serious incidents are investigated internally using a comprehensive investigation approach. Resources to support systems-based investigation in the NHS are available online from: http://www.england.nhs.uk/ourwork/patientsafety/root-cause/ **For further information relating to the circumstances and requirements for commissioning independent investigations see appendix 3.**

Level	Application	Product/ outcome	Owner	Timescale for completion
Level 1 **Concise internal investigation**	Suited to less complex incidents which can be managed by individuals or a small group at a local level	Concise/ compact investigation report which includes the essentials of a credible investigation	Provider organisation (Trust Chief Executive/relevant deputy) in which the incident occurred, providing principles for objectivity are upheld	Internal investigations, whether concise or comprehensive must be completed within 60 working days of the incident being reported to the relevant commissioner All internal investigation should be supported by a clear investigation management plan
Level 2 **Comprehensive internal investigation** (this includes those with an independent element or full independent investigations commissioned by the provider)	Suited to complex issues which should be managed by a multidisciplinary team involving experts and/or specialist investigators where applicable	Comprehensive investigation report including all elements of a credible investigation	Provider organisation (Trust Chief Executive/relevant deputy) in which the incident occurred, providing principles for objectivity are upheld. Providers may wish to commission an independent investigation or involve independent members as part of the investigation team to add a level of external scrutiny/objectivity	
Level 3 **Independent investigation**	Required where the integrity of the investigation is likely to be challenged or where it will be difficult for an organisation to conduct an objective investigation internally due to the size of organisation or the capacity/ capability of the available individuals and/or number of organisations involved (see Appendix 1 and 3 for further details)	Comprehensive investigation report including all elements of a credible investigation	The investigator and **all** members of the investigation team must be independent of the provider. To fulfil independency the investigation must be commissioned and undertaken entirely independently of the organisation whose actions and processes are being investigated.	6 months from the date the investigation is commissioned

National reporting templates should be used unless agreed that adaptions are required. National templates will be reviewed on a continuous basis. Recommendations to inform changes should be sent to england.RCAinvestigation@nhs.net

Appendix 3

TRUST LOGO

STEIS Number

Preliminary Investigation Report

Specify Type of Incident

Incident date	
Date	
Name and role of person who has compiled this report	
Name and role of Director authorising submission	
Provided to	

To be completed within 3 working dates of reporting incident

Incident Type	
Is the Incident a Never Event?	
Situation	*i.e. description of the Incident (including details of any patient harm) Background Information and basic chronology*
Location	*i.e. ward, hospital*
Responsible Clinician	
Day and Date of Incident	
Time of Day Incident Occurred	
DOB	
Lead Agency	
Name of Lead Investigating Agency	
Lead Commissioner	
Name of other Professional Stakeholders	***Include any details of police or media involvement/interest***
Communication with Patient / Relatives (ref Being Open)	***Include details of contact with or planned contact with patient/family members***
Details of other organisations/individuals notified	
Immediate Actions Taken	***Include actions taken to mitigate any further risk***
Incident Assessment: Risk Grade Identification of Care or Service Delivery Problems Reporting to External Agencies Communication Strategy	***Including level of harm that has occurred***
Recommended management plan	
Level of Investigation being undertaken	**Level 1 / Level 2 / Level 3**

Terms of Reference for the RCA Investigation The investigation team will include	
Reporting Approach / Timescale	

Serious Incident Final Report - Extension Request Form

Name & Designation of person completing this form:

Trust/Provider Name:

Date form completed:

_____

STEIS Number:

Please specify the length of extension required in number of working days (Not to exceed 20 working days:

From (Date): **To (Date):**

Reason for request (Please tick one box)**:**

Short-term sickness/absence ☐

Multi-agency involvement ☐

Other (Please specify details): ☐

Provide further details here:

Significant service change impacting on managers availability to meet deadline

---

CCG Use only

Incident report due date: **Date request received:**
Extension granted: Y / N **Number of Days:**
Date Trust/Provider informed of decision:
B/F date updated on STEIS: Y / N
Name of individual considering the extension request:
Reason for granting/refusing the extension request:

Appendix 5

Review of Serious Incident investigation report and action plan

Name of organisation: **Date:**

NUMBER	CRITERIA	YES/NO	CCG COMMENT	PROVIDER RESPONSE
1	Does the report identify the SI reference number, author and date of report?			
2	Has the report been submitted within twelve weeks from the date the incident was notified to the Federated Clinical Risk Management Team?			
3	Does the report have Chief Executive/Director sign off?			
4	Does the report give a factual description of the incident, covering the following: • Who or what was involved? • What happened? • When did it happen? • Where did it happen? • How did it happen?			
5	Does the report detail the immediate actions taken, including support to carers/staff, contact with the media and notification to external bodies?			
6	Was the investigation sufficiently robust and proportionate to the scale and complexity of the incident?			
7	Does the report identify all root causes of the incident through systematic analysis? (There may be more than one root cause) These may include: • Organisational & management factors • Work environment factors			

NUMBER	CRITERIA	YES/NO	CCG COMMENT	PROVIDER RESPONSE
	• Team factors • Individual factors • Task factors • Patient factors			
8	Does the report make robust recommendations to minimise risk of recurrence?			
9	Has the Trust developed an action plan to implement these recommendations? Are the identified actions clear and specific and resources identified where appropriate? Are there timescales set for each action? Does the report indicate the name and job title of the individual(s) responsible for each action? Are there arrangements in place to audit implementation and effectiveness of action plans?			
10	Are there any areas of good practice which have been highlighted as part of this investigation?			
11	When any new changes are made, new risks are often introduced *(e.g. bedside alcohol gel → accidental ingestion).* Have action plans been risk assessed so that any downside of the recommendations are minimised?			
12	Does the report indicate how the learning from the incident will be shared across the Trust?			
13	Is this report suitable to be shared with colleagues in an anonymised way as an exemplary report?			

Supplementary Information:
Where appropriate, has a coroner's inquest been held? If so what was the outcome?

Overview:

Further Comments:

Further information / action required:

Grading of Investigation Report
Please tick the appropriate box

Excellent		Good		Fair		Weak	

Rating	Examples of criteria
Excellent	• Report subject to a comprehensive root cause analysis • Terms of reference are clearly identified and the report follows these • Root causes and contributory factors are identified • Report contains robust recommendations and an action plan has been developed from these • Evidence based practice is detailed within the report • Details of how the learning is to be shared is contained within the report • Staff and relatives contribute to incidents where appropriate • No additional information required
Good	• Report is subject to a detailed root cause analysis investigation • Terms of reference are identified • Root causes and contributory factors are identified • Report needs minor additional information prior to closure
Fair	• Root causes not identified but contributory factors are detailed • There is no/limited monitoring/audit of actions • Report needs to be returned for additional information prior to closure
Weak	• Not subject to a RCA investigation • No terms of reference • No monitoring of action plan detailed • Report needs to be returned for substantial additional information

Grading of Action Plan
Please tick the appropriate box

Excellent		Good		Fair		Weak	

Rating	Examples of criteria
Excellent	• robust recommendations and an action plan has been developed from these • Action plan contains named leads and timescales • process in place for monitoring to ensure effective risk reduction • No additional information required
Good	• Recommendations and action plans are robust • Action plan has a named lead and timescale is provided, • Process is in place for monitoring or audit of the action plan • Report needs minor additional information prior to closure
Fair	• Recommendations and/or action plans are in place but named leads and /or timescales are not identified • There is no/limited monitoring/audit of actions • Report needs to be returned for additional information prior to closure
Weak	• Recommendations/action plan are not in place or weak • No monitoring of action plan detailed • Report needs to be returned for substantial additional information

Appendix 6

Request To Stop the Clock

Name of organisation requesting Suspension or Extension: Choose an item.			
If 'Other' please complete: Click here to enter text.			
Incident reference:	Datix Ref Click here to enter text.	STEIS No Click here to enter text.	Other Click here to enter text.
Purpose of request:	Suspension/ 'Stop the clock' ☐	Extension☐	

Please identify reason for request:

☐ Request of external body i.e. formal request by the police, a coroner or a judge

Please detail request below:
Click here to enter text.

☐ Enforced compliance with the timetable of an external agency, such as police, Coroner, Health and Safety Executive or Local Children Safeguarding Board or Safeguarding Adult Board

Please detail below:
Click here to enter text.

☐ Investigation of highly specialised and multi-organisation incidents, such as those involving a national screening programmes

☐ Incidents of significant complexity

Please detail below:
Click here to enter text.

Requesting officer:	Name: Click here to enter text.	Designation/role: Click here to enter text.
Date: Click here to enter a date.		

Request Received: (to be completed by Patient Safety Team)

Received: Click here to enter a date.		
Received by:	Name: Click here to enter text.	Designation/ role: Click here to enter text.

CCG decision:

Accepted for:	Suspension/ 'Stop the clock' ☐	Extension☐
Rationale:	Click here to enter text.	Click here to enter text.
Rejected for:	Suspension/ 'Stop the clock' ☐	Extension☐
Rationale:	Click here to enter text.	Click here to enter text.
CCG Officer:	Name: Click here to enter text.	Designation/ role: Click here to enter text.
Date: Click here to enter a date.		
Reviewed at SI Group meeting: Click here to enter a date.		
Ratified: ☐ Yes ☐N		

Appendix 7

IG incident reporting - Assessing the Severity of the Incident

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.

All IG SIRIs entered onto the IG Toolkit Incident Reporting Tool, reaching 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

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. Medium – has no effect on the base categorisation
iii. 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. Confirmed IG SIRI but no need to report to ICO, DH and other central bodies.
2. Confirmed IG SIRI that must be reported to ICO, DH and other central bodies.

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

0. Near miss/non-event

Where an IG SIRI has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a "near miss" to enable lessons learned activities to take place and appropriate recording of the event.
The following process should be followed to categorise an IG SIRI

S**tep 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.**

Baseline Scale	
0	Information about less than 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 – 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

S**tep 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	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 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 past 12 months
	Failure to securely encrypt mobile technology or other obvious security failing
	Celebrity involved or other newsworthy aspects or 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 adjusted scale indicates that the incident is level 2, the incident will be reported to the ICO and DH automatically via the IG Incident Reporting Tool.

Final Score	Level of SIRI
1 or less	Level 1 IG SIRI report via STEIS: not reportable via IG Incident Management Tool
2 or more	Level 2 IG SIRI report via STEIs but also reportable via IG Incident Management Tool

E**xample Incident Classification**

Examples	
A	Health Visitor data inappropriately disclosed in response to an FOI request. Data relating to 292 children, detailing their client and referral references, their ages, an indicator of their level of need, and details of each disability or impairment that led to their being in contact with the health visiting service e.g. autism, chromosomal abnormalities etc. Baseline scale factor 2 Sensitivity Factors -1 Limited demographic data 0 Limited clinical information +1 Particularly sensitive information +1 Parents likely to be distressed **Final scale point 3 so this is a level 2 reportable SIRI**
B	Imaging system supplier has been extracting PID in addition to non-identifying performance data. A range of data items including names and some clinical data and images have been transferred to the USA but are being held securely and no data has been disclosed to a third party. Baseline scale factor 3 (estimated) Sensitivity Factors -1 Limited demographic data 0 Limited clinical information -1 Data held securely +1 Sensitive images +1 Data sent to USA deemed newsworthy **Final scale point 3 so this is a level 2 reportable SIRI**
C	Information about a child and the circumstances of an associated child protection plan has been faxed to the wrong address. Baseline scale factor 0 Sensitivity Factors -1 No clinical data at risk 0 Basic demographic data +1 Sensitive information +1 Information may cause distress **Final scale point 1 so this is a level 1 SIRI and not reportable**
D	Subsequent to incident c the same error is made again and the recipient this time informs the Trust she has complained to the ICO.

	Baseline scale factor 0 Sensitivity Factors -1 No clinical data at risk 0 Basic demographic data +1 Sensitive information +1 Information may cause distress +1 Repeat incident +1 Complaint to ICO **Final scale point 3 so this is a level 2 reportable SIRI**
E	Two diaries containing information relating to the care of 240 midwifery patients were stolen from a nurse's car. Baseline scale factor 2 Sensitivity Factors 0 Basic demographic data 0 Limited clinical information **Final scale point 2 so this is a level 2 reportable SIRI**
F	A member of staff took a ward handover sheet home by mistake and disposed of it is a public waste bin where it was found by a member of the public. 19 individual's details were included. Baseline scale factor 1 Sensitivity Factors -1 Limited demographic data 0 Limited clinical information +1 Security failure re disposal of data **Final scale point 1 so this is a level 1 SIRI and not reportable**
G	A filing cabinet containing CDs with personal data relating to several thousand members of staff sent to landfill in error during an office move. Baseline scale factor 3 Sensitivity Factors -1 No clinical data at risk -1 Landfill unlikely to be accessed 0 Basic demographic data +1 Security failure (no encryption & poor disposal) **Final scale point 2 so this is a level 2 reportable SIRI**
H	Loss of an individual's medical records. The records were found to be missing when the patient concerned made a subject access request. Baseline scale factor 0 Sensitivity Factors 0 Basic demographic data +1 Detailed clinical information +1 Patient distressed +1 Complaint to ICO **Final scale point 3 so this is a level 2 reportable SIRI**

Definitions of Breach Types

IG Incident Reporting Users should 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. More detailed definitions are available in the IG Reporting Guidance.