NHS Lincolnshire East Clinical Commissioning Group

NHS South West Lincolnshire Clinical Commissioning Group

NHS Lincolnshire West Clinical Commissioning Group

NHS South Lincolnshire Clinical Commissioning Group

SERIOUS INCIDENT POLICY

Key words:	CG008	
Version:	1.0	
Approved by:	SLCCG Risk and Governance Committee	
Date approved:	January 2015	
Name and designation of author/originator:	Jane Christmas – reflective of regional & national guidance	
Name of responsible Committee:	Risk and Governance Committee	
Date issued for publication:	February 2015	
Review date:	October 2016	
Expiry date:	November 2017	
Target audience:	All CCG Staff; Commissioned Services	
Type of policy (tick appropriate box):	Non-clinical ☐✓	Clinical ☐
Mandatory to read?	Non-clinical staff ☐✓	Clinical staff ☐✓
Which NHSLA Risk Management Standard(s)?	Not applicable	
Which relevant CQC standards (where applicable)?	Not applicable	

1.0 Executive Summary

Serious Incident Policy

1.1 Background

Promoting Patient Safety by reducing errors is a key priority for the NHS. This responsibility was highlighted by Department of Health guidance: Organisation with a Memory (DOH 2000) and Building a Safer NHS (DOH 2001) which, collectively, emphasised the need to learn from adverse events.

The Organisation must ensure that Serious Incidents (SI's) are identified, reported and managed in an effective and timely way.

Firstly, to identify and report incidents which immediately arise or affect the Organisation, specifically to report and manage incidents related to Lincolnshire Patients.

Secondly, to review received reports from all Provider Organisations (including those external to Lincolnshire) to ensure that all appropriate action has been undertaken by the notifying Organisation, to learn and share lessons, and promote public safety and confidence.

1.2 Statement

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

1.3 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.

1.4 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.

1.5 Dissemination

The policy will be available on the Organisation website.

1.6 Resource Implications

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

Serious Incident Policy

Statement: Lincolnshire West CCG (LWCCG); East Lincolnshire CCG (ELCCG); South Lincolnshire CCG (SLCCG); South West Lincolnshire CCG (SWLCCG) are committed to the timely and effective reporting and management of serious incidents, to promote patient and organisation safety.

2.0 Background:

Promoting patient safety by reducing errors is a key priority for the NHS. This responsibility was highlighted by Department of Health guidance: Organisation with a Memory (DOH 2000) and Building a Safer NHS (DOH 2001) which, collectively, emphasised the need to learn from adverse events.

The Organisation must ensure that Serious Incidents (SI's) are identified, reported and managed in an effective and timely way.

The Organisation's role in relation to the management of Serious Incidents has been expanded as a result of devolution of responsibility from the Strategic Health Authority. The Organisation now undertakes a dual function in relation to Serious Incidents:

Firstly, to identify and report incidents which immediately arise or affect the Organisation, specifically to report and manage incidents related to Lincolnshire residents.

Secondly, to receive notification of incidents from provider Organisations, (including those external to NHS Lincolnshire). Reflecting the responsibilities of a Commissioner, ensure that all appropriate action has been undertaken by the notifying Organisation, to learn and share lessons, and promote public safety and confidence.

3.0 Definition of a Serious Incident

The definition of a Serious Incident requiring investigation is set out in the NHS England Incident Reporting framework. This is given as an **incident** that occurred in relation to **NHS-funded services and care** resulting in:

Unexpected or **avoidable** death of one or more patients, staff, visitors or members of the public

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

A scenario that prevents or threatens to prevent a Provider organisation's ability to continue to deliver health care services, for example, actual or potential loss of personal/ organisational information, damage to property, reputation or the environment, or IT failure;

Allegations of **abuse** (see sections 14 and 15 for further detail)

Potential or adverse media coverage or public concern for the organisation or the wider NHS

One of the core set of 'Never Events' as updated on an annual basis.

The NHS England Serious Incident Framework and the NPSA http://www.nrls.npsa.nhs.uk/EasySiteWeb/GatewayLink.aspx?alId=68466"Information Resource to Support the Reporting of Serious Incidents gives further guidance on what constitutes an SI and Provider Organisations should refer to this when deciding which incidents should be reported as SIs.

An incident where the patient was not harmed but required life-saving or major medical or surgical intervention because of the incident must be reported as an SI as should any SIs not previously reported where there is a Rule 43 recommendation from a Coroner.
Provider organisations should err on the side of caution, and discuss any potential SI (including near misses) with the CCG to determine if it should be reported.

4.0 The Responsibilities of LWCCG; ELCCG; SLCCG; SWCCG:

4.1 **The Commissioner** will, as part of their commissioning role, performance monitor the contract in place with all its provider organisations. They will receive from their provider's information regarding all Serious Incidents and related investigation reports. This is required to:

Inform future commissioning discussions
Ensure that questions from the public and or media can be managed appropriately
Discharge effective governance
Ensure any relevant remedial action is made as soon as possible
Ensure appropriate engagement in a joint investigation.

Throughout the year, the Commissioners will produce and review at their Quality and Experience Committees, 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.

In collaboration with Local Authorities, the CCG's have 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.

LWCCG; ELCCG; SLCCG; SWCCG 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.

LWCCG; ELCCG; SLCCG; SWCCG will additionally review and quality assure steps taken by external Provider Organisations to manage reported SIs.

Specifically, the Organisation will review the steps taken by the Provider Organisations to manage and learn from the reported incidents and will sanction the closure of the SI incident on the STEIS data base when the incident is agreed as being complete.

SIs relating to Screening, Prisons and Primary care should be reported to the lead commissioner (i.e appropriate Area Team, NHS England).

4.2 Duties:

The CCG Accountable officer has ultimate responsibility for the Serious Incident reporting process within the Organisation.

This responsibility is delegated to the CCG Executive Nurse & Quality Lead.

The wider CCG senior management team (Executive & Non – Executive Directors) will provide positive challenge and scrutiny when receiving SI reports, to enable the CCG to fully discharge its responsibilities in relation to the management of SI's.

Nominated Executive Directors will attend the SI group as required. Executive Nurse Directors (or delegated deputy) will receive notification of incidents and supported by the Clinical Risk Management Team, over see their reporting on the STEIS system and management.

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

Management and strategic over view of the SI function is delegated through the CCG Executive Nurse to the Head of Clinical Risk Management and Compliance, Federated Clinical Risk Management team.

The Clinical Risk Management and Compliance team is responsible for the risk assessment and management of all incidents reported to the Clinical Risk Management Team; for incident aggregation; trend analysis; implementation and ongoing development of the SI management process on behalf of LWCCG; ELCCG; SLCCG; SWCCG**.**

The Clinical Risk Management and Compliance team is responsible for receiving, risk assessing and managing the investigation and reporting of "own reported" SI's on behalf of LWCCG; ELCCG; SLCCG; SWCCG**.**

Nominated Root Cause Analysis (RCA) Investigation Manager(s) are 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 Nurse or Clinical Risk Management and Compliance team 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 Clinical Risk Management team.
Staff are required to complete an incident report form (IR1) 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 responsibility to consider and respond to training needs identified by their staff and to support their direct reports (in liaison with the Clinical Risk Management team) 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 Organisation Whistle Blowing process.

4.3 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.

4.4 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 LWCCG; ELCCG; SLCCG; SWCCG, on behalf of the Organisation's Governing Body.

4.5 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.

4.6 Serious Incident (SI) Group:

LWCCG; ELCCG; SLCCG; SWCCG are responsible for reviewing and closing SI's reported by Providers on the STEIS data base when satisfied that an appropriate investigation has been undertaken, when lessons learnt have been identified and an appropriate action plan developed. This function is delegated to the Executive Nurse and operationalised through the SI group.

5.0 Responsibilities of NHS Provider Organisations

5.1 Provider Organisations:

Provider Organisations have both a statutory and contractual duty to have systems in place for robust and timely management of SIs, 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 **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 co-ordinating 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).

This responsibility extends to the prompt reporting of adverse reactions and the reporting of defective products relating to medical and non medical equipment; supplies, food buildings and plant (HSG/93/13) to the appropriate agency.

NHS Provider Organisations are also responsible for ensuring that there are effective arrangements in place for dealing with major incidents (HSG/93/24); homicides allegedly committed by patients in receipt of mental health services (HSG/94/27); information governance incidents; and infection control incidents (Winning Ways, DoH 2003).

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.

6.0 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.

Where a serious incident notified includes primary care involvement, the Area team should be notified immediately. The Area Team 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:

The lead organisation co-ordinating 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 organization

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.

7.0 SIs identified in a different organisation

The NHS England Serious Incident frameworks 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. 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.

8.0 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.

9.0 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 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 a 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.

10.0 Requirements for reporting SIs to other agencies

All Safeguarding SIs should be reported to the relevant safeguarding leads as outlined in Sections 14 and 15.

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 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.

11.0 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 made the first 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 manufacture 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

12.0 Process for reporting and updating CCG's regarding SI's

12.1 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. If an organisation does not have access to STEIS, the provider should notify the Head of Clinical Risk Management (or nominated deputy) 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 Quality Lead 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.

The SI notification should indicate whether any media interest is likely. If there is immediate interest from the media the CCG Communications team should be informed immediately by the Provider Organisation's Communication team. Out of hours this should be notified to the On Call Director.

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.

12.2 Grading and retraction of SIs

The Provider should include the grade of the SI on the STEIS form. If the CCG have any queries about the assigned grade they will contact the Provider organisation within 2 working days.

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 retracted from the STEIS database rather than closed**.**

12.3 Preliminary reports

A preliminary report should be sent to the CCG within 3 days for all SIs (see appendix 2). 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.

12.4 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

13.0 Final Report Requirements

The final report can be at different levels depending on the type of SI and level of harm as outlined by the NHS England guidance (Appendix 3)

Level 1 report to be completed within 45 working days
Level 2 report to be completed within 60 working days. These include inpatient suicides; maternal deaths; never events and child protection incidents

The RCA investigation should be completed and a final report and action plan submitted within 45 days of the incident being reported for grade 1 SIs and 60 days for grade 2 SIs. This timeframe may be extended up to 26 weeks where there is an independent investigation.

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 for a Level 2 comprehensive investigation are available on the NPSA website at http://www.nrls.npsa.nhs.uk/resources/?entryid45=59847

All RCA's should have been reviewed and signed off at a senior executive level within the

provider organisation before submission. Details of who signed off the RCA must be reflected on the investigation front sheet.

14.0 Review of investigation credibility and thoroughness of final reports

All final reports will be reviewed by staff within the CCG Clinical Risk Management team. Specialist advice for reviews will be sought as required.
The CCG Executive Nurses will also review the final report to determine if all aspects of the incident have been adequately investigated. This review will usually be undertaken within the SI group led by the Clinical Risk Management Team. Further assurances will be requested as required.

15.0 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 monthly 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 Head of Clinical Risk and Compliance, 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.

16.0 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 or 'Stop the clock' date for submission would be appropriate and submit a request to the Area Team for their approval. 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. If a 'Stop the Clock' is approved, a new date for completion of investigation and submission of the final report will be agreed.

16.1 Penalties for late submission

Penalties will be attributed for the late submission of RCA's to the clinical risk management team as outlined in the Contract agreement.

17.0 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 Clinical Risk Management team will on behalf of the CCG Executive Nurse, 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 assurance tracker until sufficient assurance is received.

Progress on implementation of these action plans will be monitored via the Clinical Risk Management meetings held with providers 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.

A 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.

18.0 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.

19.0 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) produce a list of Never Events which is updated annually.

The Never events Framework -2013/14 (updated December 2013) provides the list of never events

www.england.nhs.uk/wp-content/uploads/2013/12/nev-ev-list-1314-clar.pdf

19.1 Never Events Listings

1	Wrong site surgery
2	Wrong implant/prosthesis
3	Retained foreign object post-procedure
4	Wrongly prepared high-risk injectable medication
5	Maladministration of potassium-containing solutions
6	Wrong route administration of chemotherapy
7	Wrong route administration of oral/enteral treatment
8	Intravenous administration of epidural medication
9	Maladministration of Insulin
10	Overdose of midazolam during conscious sedation
11	Opioid overdose of an opioid-naïve patient
12	Inappropriate administration of daily oral methotrexate
13	Suicide using non-collapsible rails
14	Escape of a transferred prisoner
15	Falls from unrestricted windows
16	Entrapment in bedrails
17	Transfusion of ABO-incompatible blood components
18	Transplantation of ABO incompatible Organs as a result of error
19	Misplaced naso- or oro-gastric tubes
20	Wrong gas administered
21	Failure to monitor and respond to oxygen saturation
22	Air embolism
23	Misidentification of patients
24	Severe scalding of patients
25	Maternal death due to post partum hemorrhage after elective Caesarean section

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 asses how embedded required actions are, before closure on STEIS is agreed.

20.0 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, October 2012.

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.

21.0 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 (2013) 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 Paediatrician 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 (2013) 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).

22.0 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.

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 required	Co-ordinate the collection of information about concerns - abuse or neglect that has, or may, occur. This may include an 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	Adult Safeguarding Lead and other organisations	As decided through the strategy discussion, but within 4 weeks from the alert
Safeguarding action	Analyse concerns,	Safeguarding partner	As identified from

Stage	Function	Responsibility	Time Frame
plan – development, implementation and review.	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.	organisations as appropriate	discussions, professionals meetings, strategy meeting
Serious Incident process (SI)	Provide final Adult Safeguarding documentation to SI lead in commissioning organisation 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 With in 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, ensure an investigation and final report is submitted, and monitor and report on the implementation of the improvement action plan.

22.1 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.

23.0 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 bacteraemia – all post 48 hours cases
- Any death where MRSA bacteraemia 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.

24.0 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.

25.0 Information Governance SIs involving data loss

25.1 Definition of a serious incident in relation to personal identifiable data

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, IG SIRIs could include (i) any incident involving the actual or potential failure to meet the requirements of the Data Protection Act 1998 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.

All organisations processing health and adult social care personal data are required to use the IG

Toolkit to report IG SIRIs and 'near misses'.

If you identify a possible IG SIRI you must report it on STEIS in the usual way and the incident will be assessed by the clinical risk management team. *Para 6.1 Initial Reports* refers. The clinical risk management team will also register the IG SIRI onto the HSCIC IG Incident Reporting Tool, supported by the Information Governance Lead (GEMCSU). The Information Governance Lead (GEMCSU) will provide support and offer assistance before incidents are logged onto the IG Incident Reporting Tool and provide advice and assist in any incident investigations.

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

The clinical risk management team will follow HSCIC's Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20%20IG%20SIRI%20Checklist%20Guidance_V3%200_Updated%20June%202014.pdf

Details as to whether the incident has been reported to the Information Commissioners Office (ICO) via the HSCIC IG Reporting Tool should be included on the STEIS form, data loss template and final RCA report

25.2 Assessing the severity of an IG incident

Organisations are expected to report IG Serious Incidents Requiring Investigation (SIRIs) directly to the Health and Social Care Information Centre (HSCIC) via the IG Incident Reporting Tool hosted on the secure IG Toolkit website. Further detail on the tool, how it works and how to access etc can be found in the IG Incident Reporting Tool User Guide.

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

Incidents reported will be automatically and relayed on to the ICO and other regulators, as appropriate. The severity of the incident will be determined by the scale (numbers of data subjects affected) and sensitivity factors selected. If the outcome in terms of the severity of the incident is IG SIRI level 2 (reportable) an email notification will be sent to the HSCIC External IG Delivery Team, DH, ICO and escalated to other regulators, as appropriate. If the outcome is IG SIRI level 0 or 1 no notifications will be sent. For further detail on how the severity of an incident is assessed and calculated within the IG Incident Reporting Tool, see Appendix 4

25.3 Publishing details of SIRIs in annual reports and Statements of Internal Control (SIC)

25.3.1 Principles

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

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

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

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

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

25.3.2 Content to be included in Annual Reports

Incidents classified at a IG SIRI level 2 (see Appendix 4) are those that are classed as a personal data breach (as defined in the Data protection Act) or high risk of reputational damage, basically reportable to the Department of Health and the Information Commissioner's Office.
These incidents need to be detailed individually in the annual report in the format provided. See hscic IG incident reporting guidelines for details. All reported incidents relating to the period in question should be reported, whether they are open or closed incidents.

25.4 Statement of Internal Control (SIC) Guidance

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

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

26.0 SIs relating to Pressure Ulcers

All Grade 3 and 4 pressure ulcers are SI Level 1 or 2.

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 45 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.

A template RCA is being developed, in the interim, further information regarding RCA requirements can be secured from the federated Clinical Risk Management Team.

27.0 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

27.1 Professional Misconduct

Allegations of serious professional misconduct.

27.2 Radiology

Severe equipment failure leading to harm or death.

27.3 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.

Therefore the management of a SI becomes complicated with the potential to cause delay or confusion. For this reason a policy for managing serious incidents in screening has been developed by the regional Directors of Public Health.

The policy states that a screening SI is: An actual or possible failure at any stage in the pathway of the screening service, which exposes the programme to unknown levels of risk that screening, and assessment or treatment of screen-positive people have been inadequate, and hence there are possible serious consequences for the clinical management of patients. The level of risk to an individual may be low, but because of the large numbers involved the corporate risk may be very high.

National programmes are public 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 external quality assure the screening programmes. Therefore the management of a Serious Incident becomes complicated with the

potential to cause delay or confusion. For this reason a policy for managing serious incidents in screening has been developed by the regional Directors of Public Health.

A screening Serious Incident is: An actual or possible failure of the screening service that has consequences for the clinical management of patients e.g. loss of test results, failure to detect cancers, incorrect notification of results to a patient or groups of patients. The level of risk to an individual may be low, but because of the large numbers involved the corporate risk may be very high.

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 thalassaemia
Newborn blood spot
Newborn hearing
Newborn and Infant Physical Examination

27.4 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.

27.5 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 eg 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.

27.6 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

27.7 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.

27.1 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.

28.0 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

29.0 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 Caldicott, 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.

30.0 Contact details

The contact details relating to SIs are:

Clinical Risk Management Team, LWCCG on 01522 515415

Generic in box LIWCCG.ClinicalRiskIncidents@nhs.net

31.0 References

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

Serious Incidents Requiring Investigation Policy, NHS East of England July 2010

Nursing and Midwifery Council Midwives Rules and Standards NMC 2012

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

Department of Health (October 2012). Never events policy framework. http://www.dh.gov.uk/health/2012/10/never-events

DH 'No Secrets' Guidance on developing and implementing multiagency policies and procedures to protect vulnerable adults from abuse DH 2000

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

DH Implementing a 'Duty of Candour'; A new contractual requirement on providers Analysis of consultation responses November 2012 https://www.wp.dh.gov.uk/publications/files/2012/11/summary-of-consultation-responses-duty-of-candour.pdf

NHS Commissioning Board Serious Incident Framework March 2013 - An update to the 2010 National Framework for Reporting and Learning from Serious Incidents Requiring Investigation www.england.nhs.uk/wp-content/uploads/2013/03/sif-guide.doc

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/

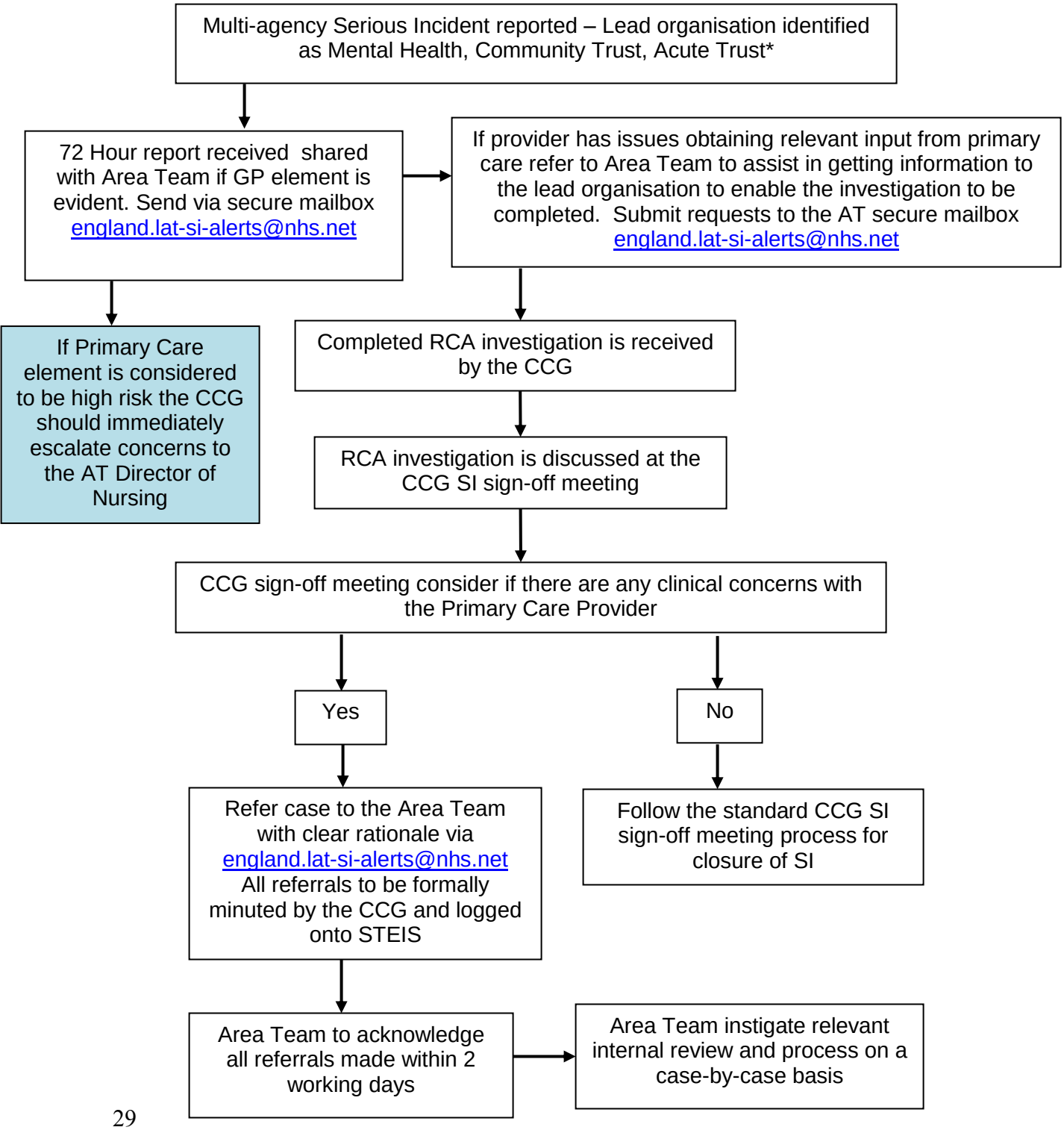
The Health and Social Care Act 2008 (Registration of Regulated Activities) Regulations 2010,

available at http://www.legislation.gov.uk/uksi/2010/781/contents/made

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

Appendix 1

Multi Agency SI Investigation Process where there is Primary Care Involvement



*Where the Primary Care element of any SI is identified as the largest proportionally the Area Team will be responsible for co-ordinating the investigation

Appendix 2
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 from Cygnet	
Provided to	**Jane Christmas**

To be completed within 3 working dates of reporting incident

Please return via safe haven fax to 01522 515365

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	
Name of other Professional Stakeholders	
Communication with Patient / Relatives (ref Being Open)	
Incident Assessment: Risk Grade Identification of Care or Service Delivery Problems Reporting to External Agencies Communication Strategy	
Recommended management plan	
Terms of Reference for the RCA Investigation The investigation team will include	
Reporting Approach /	

Timescale	

Appendix 3

NHS Commissioning Board Serious Incident Framework March 2013

Incident Grade	Example Incidents (these are suggestions, not definitive)	Investigation Grade and action	Timeframe	Commissioner responsibility
1	**Grade 1 incident examples:** Apparent suicide of people currently under the care of community mental health services. Mental health inpatient attempted suicides. Avoidable or unexplained death. Failure to meet standards for ambulance service response times, resulting in patient death/severe harm HCAI outbreaks. Grade 3 and 4 pressure ulcers. Data loss & information security (DH Criteria level 2). Adult safeguarding incident.	**Investigation Level 1** Concise root cause analysis (RCA) for incidents involving No Harm and Low Harm and/or where the circumstances are very similar to other previous incidents. In these cases it is more proportionate to use a concise RCA to ensure there are no unique factors and then focus resources on implementing improvement than conducting comprehensive investigations that will not produce new learning. These will be a small minority of cases. **Investigation Level 2** Comprehensive RCA for incidents involving moderate and severe harm or death. This should be the default level for most incidents	Following **initial** reporting within **2 working days**, the provider organisation must submit a completed investigation **within 45 working days**	Seek assurance and evidence from the provider that relevant policies and procedures are in place and implemented, for example by reviewing a sample of incident investigations and action plans as well as monitoring serious incident data trends. Close incidents after receipt of evidence demonstrating that local monitoring arrangements are in place to ensure action points are going to be implemented.
2	**Grade 2 incident examples:** Inpatient suicides (including following absconsion) Maternal	**Investigation Level 2** Comprehensive RCA (note NHS trusts should directly notify the NTDA of Grade 2 serious indcidents)	Following **initial** reporting **within 2 working days**, the provider organisation must submit a completed	Likely to involve specific assistance with and contribution to the incident response and investigation. Clo se incident after

	deaths Child protection incidents Never events Accusation of physical misconduct or harm Data loss and information security (DH Criteria level 3-5)		investigation **within 60 working days**	receipt of evidence demonstrating that each action point has been implemented is required
	Selected Grade 2 incidents: The need for independent investigations is identified and arranged by the commissioner or NHS CB, for example a major system failure with multiple stakeholders Homicides following recent contact with mental health services require an independent investigation. These will be commissioned by the relevant NHS CB area team.	**Investigation Level 3** Independent RCA (note NHS trusts should directly notify the NTDA of Grade 2 serious incidents)	Following **initial** reporting **within 2 working days** independent investigators should be commissioned to complete an investigation **within 6 months**	As for Grade 2 above but in addition, commissioning the independent investigation.

Appendix 4

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

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

Baseline Scale	
0	Information about less than 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

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Sensitivity Factors (SF) modify baseline scale **Low: For each of the following factors reduce the baseline score by 1**	
-1 for each	No clinical data at risk
Medium: The following factors have no effect on baseline score	
0	Basic demographic data at risk e.g. equivalent to telephone directory
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

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 HYPERLINK "https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf" IG Incident Management Tool

Example 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 Sensitivity Factors 2 -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 Sensitivity Factors 3 (estimated) -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 Sensitivity Factors0 -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 Sensitivity Factors 0 -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 Sensitivity Factors 2 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 Sensitivity Factors 1 -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 Sensitivity Factors3 -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 Sensitivity Factors 0 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 HYPERLINK "https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf" IG reporting guidance.