North East and North Cumbria

Corporate	ICBP046 - Serious Incidents Management Policy

Version Number	Date Issued	Review Date
1	July 2022	July 2024

Prepared By:	Senior Manager, Clinical Quality, NECS
Consultation Process:	Integrated Governance Workstream ICB Chief Nurse ICB Medical Director
Formally Approved:	July 2022
Approved By:	ICB Board

EQUALITY IMPACT ASSESSMENT

Date	Issues
March 2022	None

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3-year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.Comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1	July 2022	Senior Manager, Clinical Quality, NECS	Not Applicable. First Issue

Approval

Role	Name	Date
Approver	ICB Board	July 2022

Contents

1. Introduction

The Integrated Care Board (ICB) aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the ICB will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

The NHS treats over one million patients every single day. The vast majority of patients receive high standards of care however incidents do occur and it is important they are reported and managed effectively.

The ICB as commissioners of care seek to assure that all services which may be commissioned meet nationally identified standards, which are managed through the local contracting process. Compliance with Serious Incident (SI) and Never Event (NE) reporting is a standard clause in all contracts and service level agreements as part of a quality schedule.

The role of the ICB as commissioners is to gain assurance that incidents are properly investigated, that action is taken to improve clinical quality, and that lessons are learned in order to minimise the risk of similar incidents occurring in the future. It is intended that intelligence gained from SIs will be used to influence quality and patient safety standards for care pathway development, service specifications and contract monitoring.

The revised policy is intended to reflect the responsibilities and actions for dealing with SIs and NEs and the tools available.

It outlines the process and procedures to ensure that SIs and NEs are identified, investigated and learned from as set out in the Serious Incident Framework 2015 and the revised Never Events policy and framework 2018.

1.1 Status

This policy is a Corporate policy.

1.2 Purpose and scope

1.2.1 The purpose of this policy is to identify what is meant by a SI or NE and to describe the role of the ICB when a SI or NE occurs across a number of organisations.

This policy aims to ensure that the ICB in its commissioner role complies with current legislation and current national guidance from NHS England, in particular the reporting, notifying, managing and investigating SIs and NEs.

1.2.2 This policy applies to all employees of the ICB and is recommended for adoption by independent contractors e.g. GPs, Dental Practitioners, Optometrists and Pharmacists.

1.2.3 All NHS providers including Independent Healthcare Sector providers, where NHS services are commissioned, need to comply with the ICB reporting requirements within this policy, which reflects the Serious Incident Framework 2015 and the Never Events policy and framework 2018

2. Definitions

The following terms are used in this document:

2.1 Definition of a Serious Incident & Never Event

2.1.1 Serious incidents (SIs) are events in health care where the potential for learning is so great, or the consequences to patient, families and carers, staff or organisations are so significant that they warrant our particular attention to ensure these incidents are identified correctly, investigated thoroughly and most importantly, learned from to prevent the likelihood of similar incidents happening again. SIs can extend beyond incidents that affect patients directly and include incidents that may indirectly impact patient safety or an organisation's ability to deliver ongoing healthcare. SIs can be isolated, single events or multiple linked or unlinked events signalling systemic failures within a commissioning or health system. NHS England has produced an information resource to support the reporting and management of serious incidents which can be found in The SI Framework and supporting appendices (Appendix 1).

2.1.2 Whilst the definition of a SI is quite broad, the following criteria outline the type of incidents which should be included:

1. Unexpected or avoidable death of one or more people. This includes:
   - Suicide/self-inflicted death
   - Homicide by a person in receipt of mental health care within the recent past

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

3. 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
- Serious harm
- Actual or alleged abuse; sexual abuse, physical or psychological ill-treatment or acts of omissions which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery.

4. Never Events - all Never Events are defined as serious incidents although not all Never Events necessarily result in serious harm or death. Further information can be found in Appendix 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) the following:

    - Failures in the security, integrity, accuracy or availability of information often described as data loss and/or information governance related issues (see Appendix 3 for further information);
    - Property damage
    - Security breach/concern, Article 4 (12) of the General Data Protection Regulations "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
    - Cyber incidents: The Security of Network and Information Systems Directive ("NIS Directive") requires reporting of relevant incidents to the Department of Health and Social Care (DHSC) as the competent authority from 10 May 2018.
    - Incidents in population-wide healthcare activities such as screening or immunisation programmes where the potential for harm may extend to a large population;
    - Inappropriate enforcement/care under the Mental Health Act (1983),the Mental Capacity Act (2005) and Mental Capacity (Amendment) Act 2019: including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS or Liberty Protection Safeguards (LPS) when these come into effect replacing DOLS in 2022
    - Systematic failure to provide an acceptable standard of safe care (this may include incidents, or series of incidents, which necessitate ward/ unit closure or suspension of services); or
    - Activation of Major Incident Plan (by provider, commissioner or relevant agency)

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

an organisation.

All potential commissioner or independent contractor SIs should be reported on the Safeguard Incident & Risk Management System (SIRMS) in the first instance to be triaged for escalation via Strategic Executive Information System (StEIS), Data Security and Protection Toolkit, CareCERT etc

2.2 Working with other Organisations/Sectors

2.2.1 *Deaths in Custody*

People in custody, including those detained under the Mental Health Act (1983) or those detained under the police and justice system, are owed a duty of care by relevant authorities. The obligation on the authorities to account for the treatment of an individual is particularly stringent when that individual dies.

Any death in prison or police custody will be referred to the Prison and Probation Ombudsman (PPO) or the Independent Police Complaints Commission (IPCC) who are responsible for carrying out the relevant investigations. Healthcare providers must fully support these investigations where required to do so.

In NHS Mental Health services, providers must ensure that any death of a patient detained under the Mental Health Act (1983) is reported to the CQC without delay. However providers are responsible for ensuring that there is an appropriate investigation into the death of a patient detained under the Mental Health Act (1983) or where the Mental Capacity Act (2005) applies. In circumstances where the cause of the death is unknown and/or where there is reason to believe the death may have been avoidable or unexpected then the death must be reported to the provider's commissioner(s) as an SI and investigated appropriately.

Where the deceased is subject to a Deprivation of Liberty Safeguards (DoLS) authorisation, the coroner must always be informed, whether the death was expected or not, a coroner's officer will attend.

2.2.2 *Serious Case Reviews and Safeguarding Adult Reviews*

The Local Safeguarding Children Partnerships have the statutory responsibility to commission a Child Safeguarding Practice Review when specific criteria are met. The Local Safeguarding Adult Board now has a statutory responsibility to commission a Safeguarding Adult Review in certain circumstances.

Healthcare providers must contribute towards safeguarding reviews as requested to do so by the Local Safeguarding Partnership/Board where it is indicated that a serious incident has occurred. ICB Safeguarding Designated Professionals will provide health leadership to review processes at a local 'Place' level.

The interface between the serious incident process and local safeguarding policies must therefore be articulated in the local multi-agency safeguarding policy and protocol.

Further details on the procedure for the reporting and management of safeguarding children/adults incidents can be found in Appendix 2.

2.2.3 Domestic Homicide Reviews

Where a Domestic Homicide is identified by the police, the Community Safety Partnership (CSP) will consider whether the case meets the criteria for a Domestic Homicide Review (DHR). Healthcare providers must co-operate in this process. ICB Safeguarding Designated Professionals will provide health leadership to review processes.

2.2.4 *Homicide by patients in receipt of mental health care*

Where patients in receipt of mental health services commit a homicide, NHS England will consider and, if appropriate, commission and investigation. This process is overseen by NHS England's Regional investigation teams.

2.2.5 *Serious Incidents in National Screening Programmes*

There are a number of immunisation or screening programmes which require a broader approach to handling incidents. NHS England is responsible for the commissioning of local NHS screening services and retain responsibility for the sign-off of any SIs reported by providers in this area.

Further details on resources and guidance the management of incidents within the screening programme can be found at:

https://www.gov.uk/government/publications/managing-safety-incidents-in-nhs-screening-programmes

2.3 Information Governance and Cyber Security Serious Incidents requiring Investigation

The General Data Protection Regulation (GDPR)/UK Data Protection Bill imposes legal obligations on controllers to comply with the requirement to report specific breaches to the Information Commissioner's Office (ICO) without undue delay and no later than 72 hours of becoming aware of such a breach, where the breach is likely to result in a risk to the rights and freedoms of individuals.

The GDPR/UK Data Protection Bill requires that a controller informs individuals affected by a breach of their personal data of the breach without undue delay, where the breach is likely to result in a risk to the rights and freedoms of individuals.

Any incident involving the actual or potential loss of personal information that involves a high risk to the rights and freedoms of individuals should be considered as potentially serious and advice should be sought from the IG service.

Where an IG incident impacts upon a patient's rights and freedoms it must be reported to the Clinical Quality team so they can report it through the STEIS system as soon as possible (and no later than 24 hrs. after the incident during the working week). These must be categorised in STEIS using the "Confidential Information Leak/IG Breach" category. NHS England is responsible for notifying the Department of Health of any category 3-5 incident and will do this as soon as possible after they have been made aware of such an incident (either through STEIS or other means).

There is no simple definition of an information governance serious incident. The scope of an Information Governance Serious Incident may include:

- Breach of one of the principles of the Data Protection Act and/or the Common Law Duty of Confidentiality, or the General Data Protection Regulations.
- Unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals.

There are many possible definitions of what a Cyber incident is, for the purposes of reporting the definition is anything that could (or has) compromised information assets within Cyberspace. "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support a businesses, infrastructure and services."

These types of incidents could include:

- Phishing emails
- Denial of Service attacks
- Social Media Disclosures
- Web site defacement
- Malicious Internal damage
- Spoof website
- Cyber Bullying

NHS Digital has provided guidance for how SIs relating to information governance and cyber security should be dealt with and should be

embedded within local process and procedures. The full guidance is accessible at https://www.dsptoolkit.nhs.uk/Help/29

Individual organisations are responsible for following NHS Digital's Guide to the notification of data security and protection incidents. Incidents which score Level 2 or above must be reported centrally via the Information Governance Toolkit. If a CCG is unsure of the level of the incident, further guidance can be sought from the Commissioning Support Unit's Information Governance Team.

Breach reporting is now mandatory for all organisations. Notification and subject communication requirements will include breaches that organisations might not have notified under the previous data protection regime. The traditional view that a data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a risk to rights and freedoms of individuals under Article 33 of GDPR. 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 via this reporting tool. All personal data breaches will involve a breach of security at some point in the processing and the additional use of this tool for NIS incident reporting will save the health and social care sector time and effort in reporting.

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner when determining what the significance and likelihood a data breach will be. The significance is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest. The likelihood of the consequences occurring are graded on a scale of 1-5, 1 being a non-occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to vulnerable group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3. Further guidance can be sought from the Commissioning Support Unit's information governance team.

Consideration should always be given to informing patients/service users when person identifiable information about them has been lost or inappropriately placed in the public domain.

Loss of encrypted media should not be reported as an SI unless the data controller has reason to believe that the encryption did not meet the

Department of Health Standards that the protections had been broken or were improperly applied.

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

2.4 Serious Incidents involving controlled drugs.

SIs that involve controlled drugs must also be notified to the North of England Commissioning Support Medicines Optimisation Team and the ICB Director of Medicines.

3. Reporting & Management of Serious Incidents

3.1 Independent Healthcare sector

3.1.1 The Independent Healthcare Sector (IHS) is subject to the same contractual obligations for the reporting of SIs as other providers of NHS services. The ICB should ensure that appropriate reporting arrangements are in place with the IHS in relation to SIs where the provider is unable to directly report an SI onto StEIS (Appendix 5).

3.1.2 The commissioner of the service should ensure that IHS SIs are reported via STEIS and investigated appropriately by the responsible provider.

3.2 Provider and Commissioner Responsibilities

3.2.1 Each Provider must nominate a single point of contact or lead officer for managing their SIs.

3.2.2 Organisations should ensure that mechanisms are in place to report all incidents meeting the criteria.

3.2.3 The SI lead officer must report a SI through STEIS within 2 working days of identification of the incident as a SI, completing all relevant sections. At this stage it is important that any immediate learning and actions are included in the intitial report.

3.2.4 If appropriate, for example where a SI is likely to generate media interest, the SI lead officer must liaise with the organisation's communications team who will liaise directly NHS England Communications team. The ICB communications team should also be notified.

3.2.5 The organisation must then provide a 72hr report, which should be sent to the NECS clinical quality team responsible for the management of that provider SI caseload on behalf of the

'Place' commissioner. The report should include more information regarding the event, immediate learning and how the RCA will be conducted.

3.2.6 Under the Data Protection Act (2018) organisations need to be open and transparent with regards to investigation processes, unless there are specific exceptions. Arrangements may need to be put in place to support patients and family members through the investigation process and sharing of the outcome of investigations. The appointment of a Family Liaison Officer may be appropriate.

3.2.7 If an incident involves more than one NHS organisation, **it is the responsibility of the organisation where the incident took place** to formally report it through STEIS and to lead the investigation process. All other additional organisations involved must contribute and fully cooperate with the process in line with the agreed timescales. Where there is doubt about who should report the incident then clarity must be sought through the North of England Commissioning Support Clinical Quality Team.

3.2.8 Commissioners should help to facilitate discussions relating to who is the most
appropriate organisation to take responsibility for co-ordinating the investigation
process. Commissioners themselves should provide support in complex circumstances. Where no one provider organisation is best placed to assume responsibility for co-ordinating an investigation, the commissioner may lead this
process. The Responsible Accountable Supporting Consulted and Informed (RASCI) model should be completed in order to assign accountability and ensure lines of communication are kept open and responsibilities are clear.

3.2.9 Where an incident involves the independent sector or contracted services, it is the role of the commissioner to report the SI onto StEIS on their behalf, however responsibility for investigation remains with the provider.

3.2.10 This guidance must not interfere with existing lines of accountability and does not replace the duty to inform the police and/or other organisations or agencies where appropriate. Further guidance can be obtained from the Department of Health publication *Memorandum of Understanding: Investigating Patient Safety Incidents* June 2004 and accompanying NHS guidance of December 2006. The need to involve outside agencies should not impede the retrieval of immediate learning.

3.2.10 Certain SIs may also be subject to independent investigations conducted by the Healthcare Safety Investigation Branch (HSIB) and this includes all patient safety investigations of maternity incidents occurring in the NHS which meet criteria fokr the Each Baby Counts programme.

3.2.11 Incidents in which the actions or omissions of a provider or its employees have impacted or have had potential to impact on children and/ or vulnerable adults must be investigated in conjunction with the identified safeguarding lead and in accordance with related guidance.

3.2.12 Where an incident is subject to the involvement of a coroner, an independent inquiry, serious case review or any safeguarding issues, this should be highlighted clearly within the STEIS report as this may affect closure date.

3.2.13 Organisations should undertake investigation procedures / root cause analysis (RCA) as per organisation policy and submit to the responsible body within the agreed timescales. An example for the contents of a report and action plan can be found in **Appendix 4.** To ensure confidentiality all reports submitted to the commissioners or NECS Clinical Quality Team should be anonymous and sent via the agreed STEIS NHS-net account. NECS will conduct a quality assurance check on all RCAs on behalf of the commissioner in order to ensure the 20 day deadline is met.

3.3 Commissioner (ICB) SIs

3.3.1 If a Serious Incident has been identified as occurring within the ICB, reporters should refer to the ICBs Incident Reporting and Management Policy.

3.4 Independent Contractors

3.4.1 Once an SI is identified, in a ICB commissioned service, the Independent Contractors Procedure for the Reporting and Management of Serious Incidents should be followed, or where applicable NHS England should be notified (appendix 5).

3.4.2 Where a SI raises professional concerns about a GP, local 'Place' arrangements for assuring high standards of professional performance should be invoked, where this is applicable or NHS England notified.

3.4.3 Independent Contractors should have systems in place to ensure that staff are supported appropriately following the identification of a SI.

3.5 NHS Providers

3.5.1 Once an SI is identified, the Providers' Procedure for the Reporting and Management of Serious Incidents should be followed (appendix 6)

3.5.2 Providers should have systems in place to ensure that staff are supported appropriately following identification of a SI

3.6 Independent Healthcare Sector Providers

3.6.1 Once an SI is identified, the Procedure for the Reporting and Management of Independent Healthcare Sector Serious Incidents should be followed (Appendix 7).

3.7 Staff Involved in Serious Incidents

3.7.1 Serious incidents can be distressing for those involved.

3.7.2 The appropriate Director, Head of Service or Manager should ensure that staff are supported at all stages of a SI with reference to ICB HR policies.

3.7.3 The appropriate Director, Head of Service or Manager are responsible for ensuring that a de-briefing session occurs at an appropriate stage following a SI.

3.7.4 If, during the course of a SI investigation it becomes apparent that a member of staff may be subject to a disciplinary hearing, appropriate advice and support should be taken via Human Resources and the relevant policy followed.

3.8 Fair Blame

The ICB is committed to a policy of 'fair blame'. In particular, formal disciplinary procedures will only be invoked following an incident where:

- There are repeat occurrences involving the same person where their actions are considered to contribute towards the incident
- There has been a failure to report an incident in which a member of staff was either involved or about which they were aware (failure to comply with organisation's policy and procedure)
- In line with the organisation and/or professional regulatory body, the action causing the incident is removed from acceptable practice or standards, or where
- There is proven malice or intent

Fair blame means that the organisation:

- Operates its incident reporting policy in a culture of openness and transparency which fulfils the requirements for integrated governance
- Adopts a systematic approach to an incident when it is reported and does not rush to judge or 'blame' without understanding the facts surrounding it
- Encourages incident reporting in the spirit of wanting to learn from things that go wrong and improve services as a result

3.9 Information for Education and Training Organisations

3.8.1 In the event an incident involves a student or trainee, the relevant academic institution will be notified by the NHS Trust/ICB as appropriate.

3.8.2 Where a SI concerns the commissioning or provision of medical or dental education or training, or a medical or dental trainee or trainees, there will be appropriate communication between the ICB and Health Education England (North East).

3.9 ICB Management & Closure of Serious Incidents

3.9.1 The ICB is responsible for quality assuring the robustness of its providers' serious incident investigations and the action plan implementation undertaken by their providers.

3.9.2 The ICB is responsible for evaluating investigations and gaining assurance that the processes and outcomes of investigations include identification and implementation of improvements that will prevent recurrence of serious incidents.

3.9.3 In order to achieve this, the ICB has established the Serious Incident Panel and the terms of reference can be found in Appendix 8.

4. Implementation

4.1 This policy will be available to all Staff for use in the circumstances described on the title page.

4.2 ICB directors and managers are responsible for ensuring that relevant staff within the ICB have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

4.3 The implementation of the detail of this policy is aligned into the full roll-out, development and implementation of the incident module of the SIRMS across the ICB and NECS.

4.4 This policy is reviewed at regular intervals to ensure that the implementation of the processes contained in the policy are in line with the practical experience of users of the SIRMS.

5. Training Implications

5.1 The sponsoring director will ensure that the necessary training or education needs and methods required to implement the policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

5.2 The level of training required in incident reporting and management varies depending on the level and responsibility of the individual employee.

5.3 The training required to comply with this policy is key to the successful implementation of the policy and embedding a culture of incident reporting and management in the organisation. Through a training and education programme, staff will have the opportunity to develop more detailed knowledge and appreciation of the role of incident reporting and management. Training and education will be offered through a rolling programme of incident reporting and management training.

6. Documentation

6.1 Other related policy documents.

- Serious Incident Framework (March 2015)
- Revised Never Events Policy and Framework (March 2015)

6.2 Best practice recommendations

- Managing Safety Incidents in National Screening Programmes (October 2015)
- Health and Social Care Information Centre; Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation

7. Monitoring, Review and Archiving

7.1 **Monitoring**

The ICB Board will agree with the Chief Executive a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

The Executive Director will ensure that each policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

7.2 **Review**

7.2.1 The ICB Board will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. **No policy or procedure will remain operational for a period exceeding three years without a review taking place.**

7.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Executive Director will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

7.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the ‘document history’ table on the front page of this document. **(**

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

7.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice 2021.

Annex A

Schedule of Duties and Responsibilities

Through day to day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to the CFS or the chief finance officer immediately.

ICB Board / ICB Quality/Governance/Safety Committee	Has delegated responsibility to the ICB Board for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Accountable Officer	The accountable officer has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements. The Chief Officer has responsibility for ensuring that the ICB has the necessary management systems in place to enable the effective management and implementation of all risk management and governance policies and delegates the responsibility for the management of SIs to the Executive Director of ?Nursing?
Senior Clinical Quality Manager	The *Senior Clinical Quality Manager, NECS,* will ensure that the policy is updated according to the agreed timetable for review, or whenever significant changes occur in the statutory frameworks governing it
Commissioning Support Staff.	Whilst working on behalf of the ICB NECS staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation
Clinical Quality Team (NECS)	Will ensure that the Serious Incident Policy is implemented operationally and according to the internal Standard Operating Procedures governing the use of StEIS, SIRMS and other systems and processes to enable the effective administration and management of all SIs.

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

Annex B

Equality Impact Assessment

Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Gregor Miller
Job Title: Senior Clinical Quality Manager
Organisation: NECS

Title of the service/project or policy: ICB Serious Incident Policy

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:
This policy aims to ensure that the ICB as Commissioners comply with current legislation as well as current national guidance, NHS England guidance and requirements with regard to accident/incident reporting generally, but in particular reporting, notifying, managing and investigating Serious Incidents and Never Events.

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations** ☒
- **Voluntary / Community groups / Trade Unions** ☐

- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

No detrimental impact identified

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: Click here to enter text.		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Click here to enter text.	Click here to enter text.	Click here to enter text.

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

Appendix 1

SERIOUS INCIDENT FRAMEWORK 2015/16 & FREQUENTLY ASKED QUESTIONS

Serious Incident Framework 2015
https://www.england.nhs.uk/patient-safety/serious-incident-framework/

Serious Incident Framework 2015 FAQs

Never Events Policy and Framework 2018
https://improvement.nhs.uk/documents/2265/Revised_Never_Events_policy_and_framework_FINAL.pdf

Never Events List 2018
https://improvement.nhs.uk/documents/2266/Never_Events_list_2018_FINAL_v5.pdf

Never Events Policy Framework FAQs

Appendix 2

PROCEDURE FOR THE REPORTING AND MANAGEMENT OF SAFEGUARDING CHILDREN/ADULTS INCIDENTS

Link to, or embedded policy/procedure document for ICB Safeguarding SOP

Appendix 3

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Reportable Incidents

It is essential that all Information Governance reportable data security and protection incidents which occur in Health, Public Health and Adult Social Care services are reported appropriately and handled effectively.

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

- The management of reportable IG incidents conforms to the processes and procedures set out for managing all Serious Incidents Requiring Investigation as well as the NHS Digital Guide to the Notification of Data Security and Protection Incidents;
- There is a consistent approach to evaluating IG reportable incidents;
- The ICO must be notified of all reportable Incidents within 24 hours of becoming aware of them;
- Any affected data subjects / individuals are appropriately informed;
- Early reports of reportable incidents are sufficient to decide appropriate escalation, notification and communication to interested parties;
- Appropriate action is taken to prevent damage to patients, staff and the reputation of Healthcare, Public Health or Adult Social Care;
- All aspects of a reportable incident are fully explored and 'lessons learned' are identified and communicated; and
- Appropriate corrective action is taken to prevent recurrence
- Caldicott 2 recommendations (accepted by the Government) are addressed.
- The National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs standards are met;
- There is transparent reporting of incidents
- Contractual obligations are adhered to with regards to managing, investigating and reporting reportable incidents in a standardised and consistent manner, including reporting to Commissioners.

Appendix 4

EXAMPLE TEMPLATE

Guidance on Serious Incident Report and Action Plan

The report into Serious Incidents and the associated action plan should cover the following minimum information. Further work is under way with local organisations to develop and agree a common template

Report

- Introduction
- Constitution and investigation procedure
- Membership of the investigation team
- Terms of reference
- Background information
- Chronology
- Findings – to be identified against each of the terms of reference
- Conclusions
- Root cause(s)
- Lessons learnt
- Recommendations

Action Plan

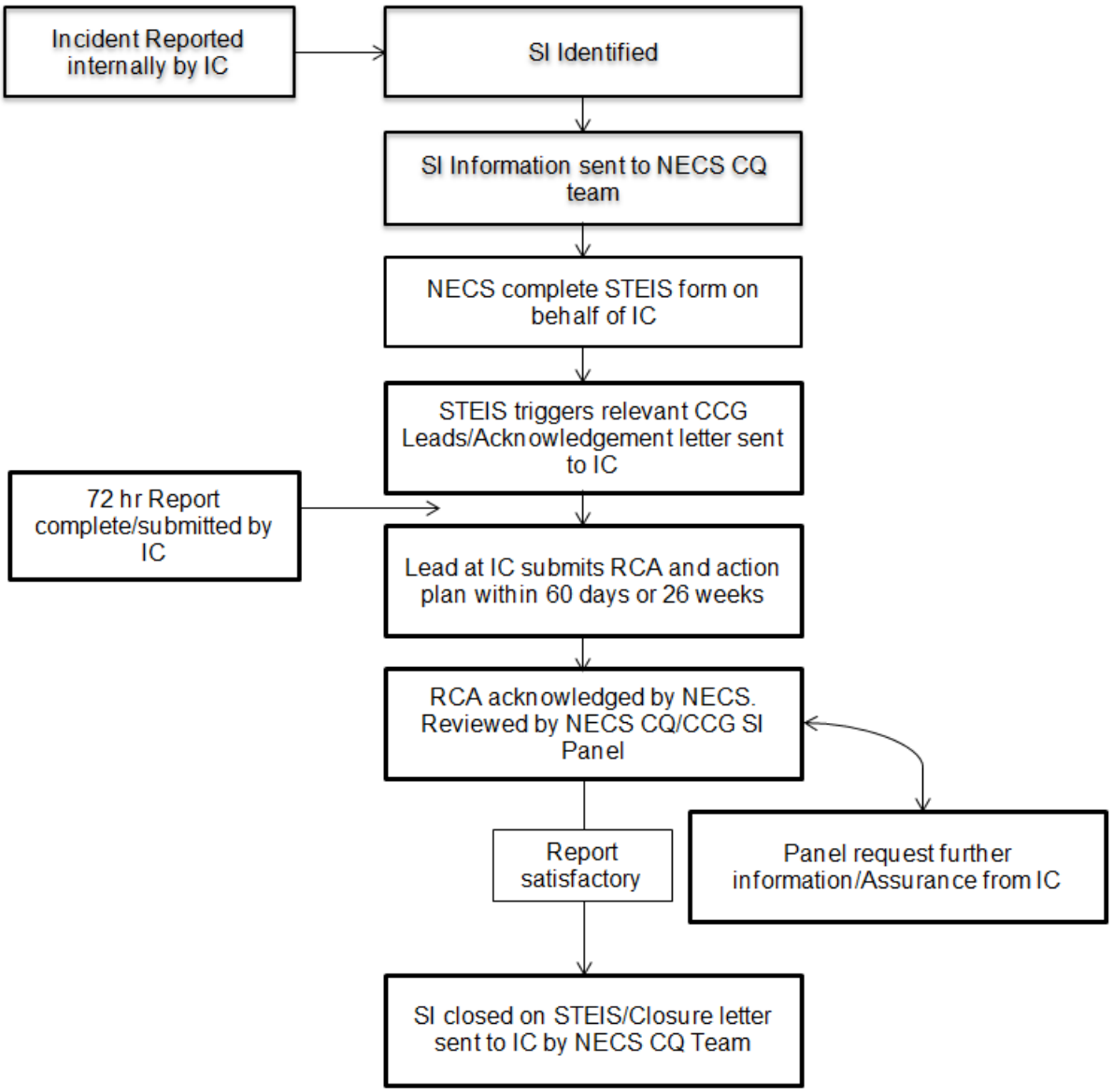
- Clearly set out which fall from the recommendations
- What needs to happen to achieve the outcome
- Identified title of who is responsible for the action
- Specific timescales on-going except where incorporated in to the Trust's everyday business for example the organisations annual programme of audit.

Root cause analysis tools to assist organisations in their investigation can be found at:

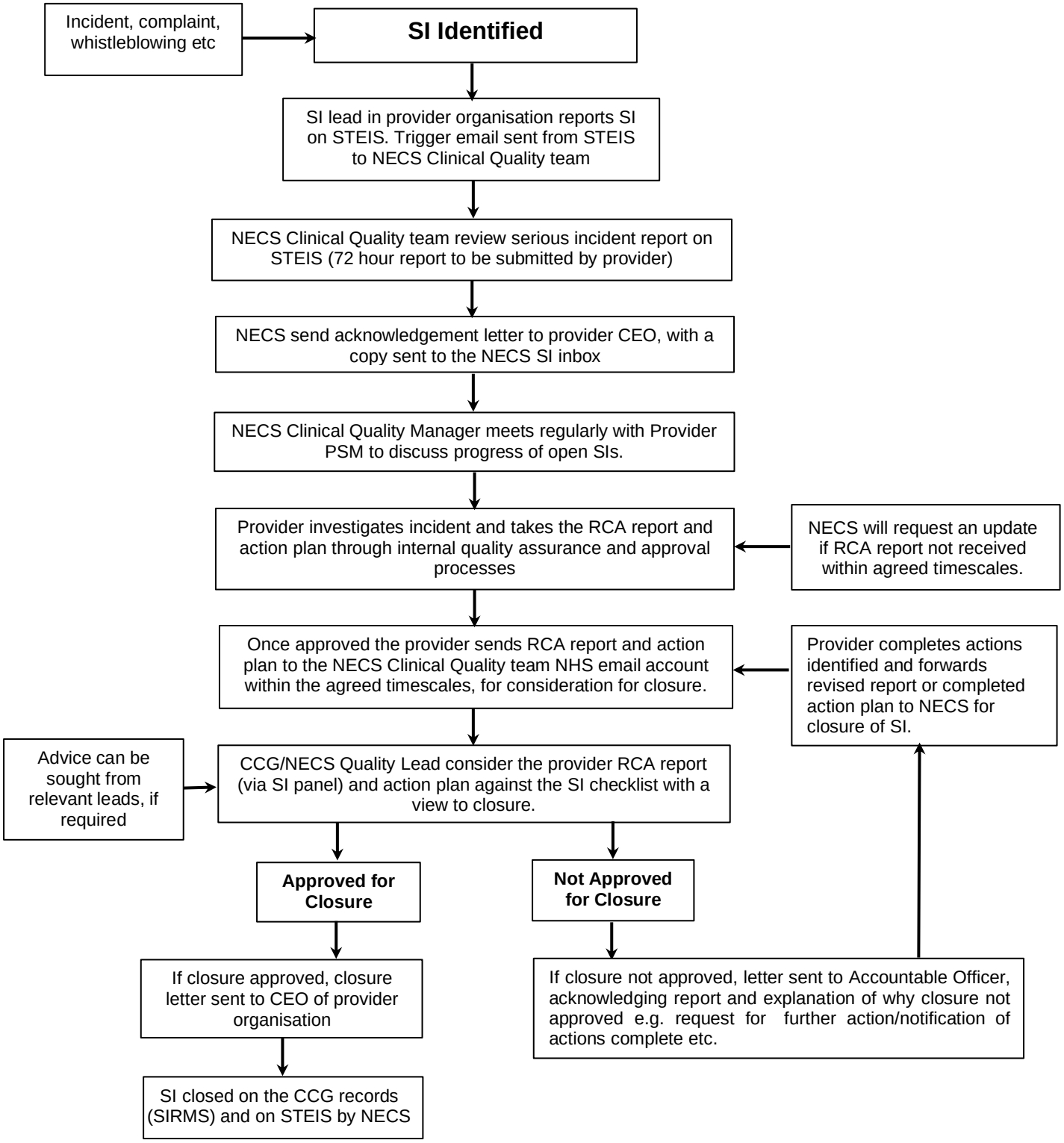
http://www.nrls.npsa.nhs.uk/resources/collections/root-cause-analysis/

Appendix 5

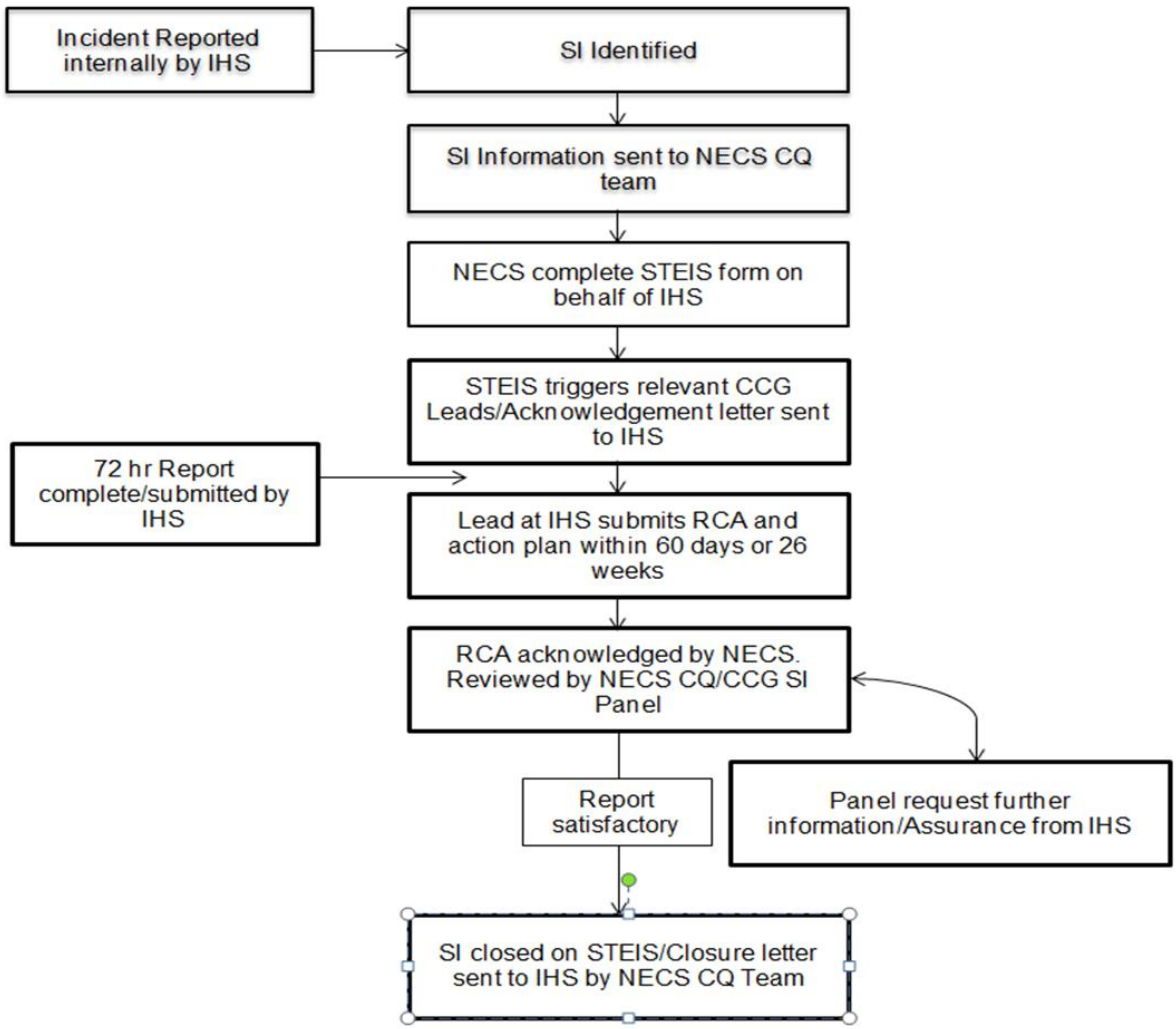
Procedure for the Reporting and Management of Independent Contractor/Commissioned Service SIs Only



Appendix 6
Procedure for the Reporting and Management of NHS Provider SIs Only



Appendix 7 Procedure for The Reporting And Management Of Serious Incidents Independent Healthcare Sector (IHS) Providers



Appendix 8

Serious Incident Review Panel
Terms of Reference

To be determined