## Incident Reporting and Management Policy

<table>
<thead>
<tr>
<th>Ratified</th>
<th>Governance &amp; Risk Committee &lt;13/05/15&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Issued</td>
<td>10/02/2015</td>
</tr>
<tr>
<td>Approved By</td>
<td>Governance and Risk Committee</td>
</tr>
<tr>
<td>Consultation</td>
<td>Governance Team, NECs</td>
</tr>
<tr>
<td></td>
<td>Clinical Quality Team NECS</td>
</tr>
<tr>
<td></td>
<td>Customer Relation Manager NECS</td>
</tr>
<tr>
<td></td>
<td>Business information Services NECS</td>
</tr>
<tr>
<td></td>
<td>North of England CCGS</td>
</tr>
<tr>
<td>Equality Impact Assessment</td>
<td>Completed</td>
</tr>
<tr>
<td>Distribution</td>
<td>All Staff</td>
</tr>
<tr>
<td>Date Amended following initial ratification</td>
<td>NA</td>
</tr>
<tr>
<td>Implementation Date</td>
<td>June 2015</td>
</tr>
<tr>
<td>Planned Review Date</td>
<td>June 2018</td>
</tr>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Author</td>
<td>Senior Governance Officer,</td>
</tr>
<tr>
<td></td>
<td>North of England Commissioning Support Unit</td>
</tr>
<tr>
<td>Reference No</td>
<td>CO08</td>
</tr>
</tbody>
</table>

### Policy Validity Statement
Policy users should ensure that they are consulting the currently valid version of the documentation.
1. **Version Control**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Author</th>
<th>Update comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>28/02/2013</td>
<td>Governance Lead, NHS South of Tyne and Wear.</td>
<td>Policy adopted by Clinical Commissioning Group (CCG) as part of policy suite developed by NECS.</td>
</tr>
<tr>
<td>V2</td>
<td>05/02/2015</td>
<td>Senior Governance Officer, NECS</td>
<td>Annual Review</td>
</tr>
<tr>
<td>V3</td>
<td>30/04/2015</td>
<td>Senior Governance Manager, NECS</td>
<td>Annual Review (amendments)</td>
</tr>
</tbody>
</table>

2. **Approval**

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and Risk Committee</td>
<td>Simon Gregory, Chief Finance Officer, STCCG</td>
<td>14 August 2014</td>
</tr>
<tr>
<td>Governance and Risk Committee</td>
<td>Simon Gregory, Chief Finance Officer, STCCG</td>
<td>13 May 2015</td>
</tr>
</tbody>
</table>

3. **Review**

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.
## Contents

1. Introduction ........................................................................................................... 5

2. Status .................................................................................................................... 6

3. Purpose and scope .................................................................................................. 6

4. Definition of an Incident ...................................................................................... 7

5. Incident Reporting ............................................................................................... 7

   5.1 How to report a CCG incident ......................................................................... 7
   5.2 Where to record your incident on SIRMS: .................................................... 7
   5.3 What to report .................................................................................................. 8

6. Management of CCG Incidents ............................................................................. 8

   6.1 Investigation of Incidents ................................................................................ 9
   6.2 Investigation of Serious Incidents (SIs) .......................................................... 9
   6.3 Information Governance (IG) and Information Technology (IT) Serious Incidents .... 10
   6.4 Health and Safety/Fire/Security/Environmental, Serious Incidents - RIDDOR Reportable 10
   6.5 Clinical Incidents ............................................................................................ 11
   6.6 Corporate Business Serious Incidents ............................................................. 11
   6.7 Fraud and Corruption Serious incidents ......................................................... 12

7. Trend Analysis /Learning Lessons ....................................................................... 12

   7.1 Internal Reporting of Incidents ..................................................................... 12
   7.2 Levels of Investigation .................................................................................. 12
   7.3 Onward Reporting .......................................................................................... 13

8. Duties and Responsibilities .................................................................................... 14

9. Implementation ....................................................................................................... 15

10. Training Implications .......................................................................................... 16

11. Fair Blame ............................................................................................................. 16

   11.1 Support for staff, and others ....................................................................... 16
12.0 Documentation .............................................................................................................. 17
12.1 Other CCG Related Documents .................................................................................... 17
12.2 NHS policy, legislation and statutory requirements ....................................................... 17
12.3 References .................................................................................................................... 17

13.0 Monitoring, Review and Archiving ................................................................................. 18
13.1 Monitoring .................................................................................................................... 18
13.2 Review .......................................................................................................................... 18
13.3 Archiving ....................................................................................................................... 18

14. Equality Analysis .............................................................................................................. 19

Appendix 1 .......................................................................................................................... 20
Appendix 2 .......................................................................................................................... 24
Appendix 3 .......................................................................................................................... 26
Appendix 4 .......................................................................................................................... 28
Appendix 5 .......................................................................................................................... 31
Appendix 6 .......................................................................................................................... 34
Appendix 7 .......................................................................................................................... 37
Appendix 8 .......................................................................................................................... 40
Appendix 9 .......................................................................................................................... 47
Appendix 10 .......................................................................................................................... 49
Appendix 11 .......................................................................................................................... 51
1. Introduction

The Clinical Commissioning Group (CCG) aspires to the highest standards of corporate behaviour and clinical competence, to ensure safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients and their carers, the public, staff, stakeholders and use of public resources. In order to provide clear and consistent guidance, CCG will develop documents to fulfil all statutory, organisational and best practice requirements.

The organisation has a responsibility for managing incidents to ensure the quality of the services it commissions are safe and of a high standard. The CCG has a responsibility to ensure their contractors have effective systems in place to identify and manage incidents and risks and support them in their development where necessary.

In our duties as a CCG we are required to act as a conduit for information about such risks and incidents and to ensure that the learning (and the opportunities for risk reduction) from them is not lost within the CCG or the wider NHS. This policy sets out the CCG’s approach to the management of incidents in fulfilment of its strategic objectives and statutory obligations.

The reporting of incidents will help the CCG identify potential breaches in its core business including breaches in:

- contractual obligations;
- internal processes;
- performance targets;
- service specifications etc.;
- statutory duties.

This policy will enable the organisation to learn lessons from adverse events and supports implementation of action to prevent incidents reoccurring. Reported incidents will be periodically analysed and results will be shared with departments and stakeholders where appropriate. The reporting and management process uses a root cause approach to analyse incidents.

The CCG aims to develop an open learning culture of incident reporting, based on the principles of fair blame.

This policy has broadly been categorised as follows:

- corporate business incident;
- clinical incidents;
- fraud and corruption;
- health and safety/ fire/ security or environmental incidents;
- information governance incidents;
- I.T (Information Technology) Incidents and cyber security.

The policy framework interlinks with CCG CO18 Serious Incidents (SIs) Management Policy guidance for the reporting and management of serious incidents.
The adoption and embedding within the organisation of an effective integrated incident management framework will ensure that the reputation of the CCG is maintained, enhanced, and its resources used effectively to ensure business success, financial strength and continuous quality improvement in its operating model.

2. Status

This is a corporate policy which outlines the Incident Reporting and Management Framework for South Tees CCG.

3. Purpose and scope

This policy provides information and guidance to staff working within the CCG to report incidents and near misses. This will be achieved by:

- providing guidance on the process for reporting and managing incidents to CCG employees and contractors;
- setting out the roles and responsibilities of CCG employees, contractors, committees and the organisation as a whole in the reporting and management of incidents;
- outlining the principles that underpin the organisation’s approach to incident reporting and management;
- providing clear definitions of the terminology within incident reporting and management, to ensure that no confusion exists between historical and current terms;
- providing clear guidance to employees of the organisation as to the kinds of incidents and issues that can be reported within the system;
- providing a clear organisational position on the principles of investigation used when responding to incidents, including fair blame and root cause analysis;
- outlining how actions, outcomes, trends and lessons learned from incidents will be monitored and reviewed;
- providing information and guidance on how the organisation aims to meet the requirements for onward reporting of incidents to the National Reporting and Learning System (NRLS);
- integrating where relevant the existing organisational policy for Serious Incidents (SIs) “CCG Policy and Procedure Guidance for Reporting and Management of Serious Incidents (SIs)”;
- providing a clear description of the reporting and management process based on the tools available (SIRMS), to ensure that all of the above can be achieved.
4. **Definition of an Incident**

An incident is a single distinct event or circumstance that occurs within the organisation which leads to an outcome that was unintended, unplanned or unexpected.

The incident could also occur outside the organisation if a member of staff is visiting other locations in the course of their work. Incidents are often negative by nature but can also include positive leaning events which can be shared throughout the organisation as good practice.

An incident could involve:

- environment (workplace);
- organisational reputation;
- property;
- service delivery;
- staff;
- stakeholder.

The incident might impact on different aspects of CCG operations for example:

- our reputation;
- our resources;
- our staff;
- the quality of services.

5. **Incident Reporting**

Every CCG employee must ensure that any incident that they are involved in, witness or become aware of is reported either by themselves or another person. Specific employee responsibilities under this policy are described in section 8 of this document.

The reporting of incidents and near-misses is a key element in the governance of the organisation. Having a system that enables the capture and analysis of incident information is the cornerstone to effective risk management and can assist in the learning of lessons, prevention of harm and improvement of performance.

5.1 **How to report a CCG incident**

Employees and contractors who have access to the staff intranet have access to the electronic on-line reporting system SIRMS (Safeguard Incident and Risk Management System). This is the preferred method for reporting incidents in the organisation. For the vast majority of staff, SIRMS can be accessed at this web-address:

https://sirms.necsu.nhs.uk

Full guidance on how to report an incident via the web-form can be found in the SIRMS web-form reporting guide and the SIRMS incident management guide (appendix 2 and 3). If there are any difficulties accessing the web-form please contact a member of the CSU SIRMS team. The SIRMS team can be contacted via email: NECSU.SIRMSINCIDENTS@nhs.net

5.2 **Where to record your incident on SIRMS:**
All CCG Staff (permanent, fixed term and contractors) have a duty to report clinical and non-clinical incidents they are involved in or witness:

- All CCG incidents should be recorded by CCG staff on the SIRMS CCG/GP incident page.

All Information governance incidents must be treated in accordance with NHS England information and Security Incident Reporting Procedure.

5.3 What to report

All employees of CCGs have a duty to report all incidents that they are directly involved in or have an awareness of. This can mean the reporting of incidents most commonly associated with incident reporting such as slips, trips/ falls, road traffic accidents or information governance breaches, corporate business incidents and I.T.

The types of incidents reported by CCG staff broadly fall into the following categories:

- corporate business incidents;
- clinical incidents;
- health and safety Incidents fire/ security or environmental Incidents;
- information governance/cyber security incidents;
- fraud and corruption;
- I.T (Information Technology) Incidents.

6.0 Management of CCG Incidents

The maintenance and the administration of the incident reporting system is largely the responsibility of the Governance Team within the CSU Organisational Development and Corporate Services Directorate. The operational management of specific incidents is the responsibility of the CCG:

- Corporate Governance & Risk Officer;
- CCG Incident Investigating Manager;
- The specialist manager relating to the type of incident reported.

The SIRMS incident reporting tool operates an email notification system within which the CCG Corporate Governance & Risk Officer is informed of the incident when submitted by CCG staff.

It is the responsibility of the CCG Corporate Governance & Risk Officer to identify who is the most appropriate person to follow up the incident/email notification and fill in the related management action form which ensures ownership of the:

- management of the incident;
- management of risks associated with the incidents;
- action taken to mitigate further risk;
- the implementation of action to address any lessons learned.

The following flowcharts outline the process managers should follow to manage CCG incidents:

a. Corporate business Incident (appendix 4)
b. Health and Safety/Environmental/Security (appendix 5)
c. Information Governance and IT Incident (appendix 6)
d. Patients Safety Clinical Incidents (appendix 7)
e. Incident Risk Matrix (appendix 8)
f. Incident management checklist: (appendix 9).

6.1 Investigation of Incidents

Where incidents are sufficiently serious or complex, or part of an ongoing pattern, a formal investigation may need to take place to establish the root cause of the incident.

The level of investigation guided by the level of risk presented by the reported incident should be measured as part of the reporting procedure by both the reporter and the incident investigating manager. However it should be noted that as individual incidents can vary so too can the level of investigation required.

The standard approach to the investigation of any incident occurring within the organisation is to apply the principles of a Root Cause Analysis (RCA) to establish the true reasons for the incident so they may be prevented in the future. Refer to the following hyperlink for RCA guidance (appendix10).

In practical terms, any incident that takes place will usually generate a volume of paperwork related to its investigation and management. The SIRMS system enables users to attach electronic documents to the individual incident files. Once incidents are reported onto the SIRMS system, managers are encouraged to use the system as an archive for key documents and information related to the incident, for example, investigation reports, meeting notes or risk assessments.

6.2 Investigation of Serious Incidents (SIs)

In some cases the outcome of an incident is such that it is immediately obvious that the incident is serious. In this instance the serious incident should be immediately reported to the Chief Officer and the Chief Finance Officer. To help you assess the risk score of a CCG incident, the reporter should use the incident risk matrix (appendix 8). The matrix demonstrates the criteria for scoring the consequence of the incident (which indicates the seriousness of the incident).

A consequence score of 5 (catastrophic) or 4 (high risk) indicates the incident is serious and this should be reported immediately to the Chief Officer and Chief Finance Officer.

A management response is required as soon as possible within a 24 hour period. These incidents need to be reported verbally if possible and recorded immediately on SIRMS.

The CSU Clinical Quality Team is responsible for recording CCG serious incidents on to the Strategic Executive Information System (STEIS). Not all CCG serious incidents will be STEIS reportable, but to ensure each serious incident is given due attention SIRMS will immediately trigger all CCG reported serious incidents to the “Clinical Quality Teams” generic email box for consideration.

An incident involving the use of personal confidential data is defined as “an incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals”. This should be considered as serious.
6.3 Information Governance (IG) and Information Technology (IT) Serious Incidents

All organisations processing health and adult social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the DH, ICO and other regulators.

Where it is suspected that an IG SIRI or cyber-incident has taken place, the Chief Officer, SIRO, Caldicott Guardian and Corporate Governance and Risk Officer should be informed. The CSU Senior Governance Manager for Information Governance and Head of Communications should also be notified.

For information governance there is no simple definition of a serious incident. 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 an IG/IT serious incident could be any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1981 and/or the Common Law Duty of Confidentiality. This includes:

- unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people’s privacy;
- such personal data breaches which could lead to identity fraud or have other significant impact on individuals;
- applies irrespective of the media involved and includes both electronic media and paper records.

As there is no simple definition for an IG a serious incident, the IG team will quality check daily CCG incidents recorded on SIRMS to determine if the recorded incident is reportable as a SIRI (Serious Incidents Requiring Investigation) to the DH (Department of Health), the ICO (Information Commissioning Officer). The Health and Social Care Information Centre (HSCIC) IG Toolkit is used to make this assessment. The NECS IG Team will assist the CCG in making this assessment and reporting SIRI’s appropriately.

Examples of information security incidents:

- using another user’s login id;
- unauthorised disclosure of information;
- leaving confidential / sensitive information unsecure;
- theft of IT equipment;
- accessing a persons’ record inappropriately e.g. viewing your own health record or family members, neighbours, friend etc.
- sharing a smartcard;
- misuse of email / internet;
- installing unauthorised software;
- threat of cyber security.

6.4 Health and Safety/Fire/Security/Environmental, Serious Incidents - RIDDOR Reportable
The organisation is statutorily obliged to report RIDDOR (Report of Injuries, Diseases and Dangerous Occurrences REGS, 1995) incidents to the Health and Safety Executive. Incidents must be reported to RIDDOR when someone has been absent from work for more than 7 days due to an incident. The CSU Health and Safety Specialist will report the incident to the H&S Executive. If the incident recorded falls in to this category staff should email your NECS Health and Safety Specialist at: necsu.healthandsafety@nhs.net and advise accordingly.

6.5 Clinical Incidents
A clinical incident occurs when one of more patients are harmed or potentially harmed. It is expected that this type of incident will not often occur in a CCG organisation as they do not provide Clinical Services. Staff (permanent, fixed term and contractors), have a duty to report any clinical incidents that they witness or are involved in. To report these staff are instructed to use the CCG/GP. Reporting an incident page of SIRMS - https://sirms.necsu.nhs.uk/

The NECs Clinical Quality Team leads in the management of patient safety clinical incidents in CCGs and GP member practices. The team is responsible for recording serious incidents on STEIS. Not all serious incidents will be STEIS reportable, but to ensure each serious incident is given due attention SIRMS automatically triggers all CCG reported serious incidents to the Clinical Quality Teams Generic email box.

The Clinical Quality Team will consider if the serious incident falls into the category of a STEIS reportable SI and report accordingly using guidance found in the CCG Policy and Procedure Guidance for Reporting and Management of Serious Incidents (appendix11)

CCG’s are required to report incidents that have a direct consequence on the safety of patients to the NRLS (National Reporting and Learning System), this is a clinical quality team function.

SIRMS is configured to escalate incidents to the clinical quality team in line with the serious incident policy.

6.6 Corporate Business Serious Incidents
A corporate business incident is a business event or circumstance that could have or did have a negative impact on the organisation, its stakeholders or the services in which it commissioned.

The CCG, as commissioners, seek to assure that all services they commission or directly provide meet national identified standards, and to ensure that this is managed through their contracting process. Compliance with serious incident (SI) reporting is a standard clause in all CCG contracts and service level agreements as part of the quality schedule.

The impact of a business incident is likely to have led to a financial loss or a negative impact on the reputation of the business.

A business incident that is reportable might include one or more of the following:

- a lack of capacity or a service gap in meeting commissioning responsibilities;
- a quality concern;
- a communications breakdown.
An overview of CCG corporate business incident trends, themes and lessons learnt will be reported to the Governance and Risk Committee four times each year. The CCG will ensure its Business Continuity Plan is amended to reflect the lessons learned from an incident where appropriate.

6.7 Fraud and Corruption Serious incidents

All cases of suspected fraud or corruption should be notified immediately through the CCG Chief Finance Officer who will give advice and arrange investigation of the incident in accordance with the CCG Standing Financial Instructions.

The CCG Chief Finance Officer maintains oversight of suspected economic crime referrals and the progress of subsequent enquiries. Cases will be referred to the Police only by the Chief Finance Officer / Local Counter Fraud Service (LCFS) or NHS Area Anti-Fraud Specialist.

Liaison will be managed by the parties involved, on a case by case basis, with reference to NHS Protect / ACPO Memorandum of Understanding and any relevant Police Divisional Policy conditions.

South Tees CCG C006 Anti-Fraud Policy (2015) outlines the CCG’s responsibilities in delivering a comprehensive approach to ensure that all suspected economic crime is referred appropriately in accordance with specified reporting lines, and that substantiated enquiries are always conducted solely by professionally accredited NHS Counter Fraud Specialists or the Police. This policy applies to all CCG employees, as well as consultants, vendors, contractors, and/or any other parties who have a business relationship with the CCG.

7.0 Trend Analysis /Learning Lessons

7.1 Internal Reporting of Incidents

SIRMS is capable of producing a range of reports based on all of the information fields and variables present on the SIRMS incident reporting/management system at regular intervals. These reports can be tailored to the specific needs of the organisation via directorates, teams or committees. They can be used to feedback information on trends, learnt lessons and actions taken. Requests for specific tailored reports can be made to NECs Governance Team - https://sirms.necsu.nhs.uk/

An overview of incidents reported across the organisation will be monitored quarterly for trends, themes and lessons learnt by the Governance Audit and Risk Committee.

7.2 Levels of Investigation

It is the responsibility of the CCG to ensure that an appropriate investigation take place follows an incident or near miss according to the severity and possible implications of the incident. It is important to note that:

- all losses and compensations must be investigated;
- all potential claims and complaints must be investigated.
If the incident occurred within a different organisation, the incident must still be reported for appropriate investigation and a decision made as to the most appropriate lead for the investigation.

Incidents with an impact assessment of 1 to 3 may not require further action other than that specified in the initial incident form. Reassessment of any residual risk must be carried out after the implementation of any actions. For incidents with an impact of assessment of 4 or 5 an investigation must always be carried out.

7.3 Onward Reporting

Occasionally, CCG will be required to onward report trends and lessons learnt for certain categories of incidents to other organisations.

All serious incidents are initially reported through SIRMS. These incidents are then escalated via SIRMS to the appropriate team/contact person responsible for managing external reporting for:

- NRLS: national reporting and learning system
- STEIS: strategic executive information system
- SIRI: serious incidents requiring investigation
- RIDDOR: report of injuries, diseases and dangerous occurrences
- HSE: the health and safety executive
- ICO: the information commissioning officer
- NHS Protect: protection against fraud and corruption in the NHS.

SIRMS can tailor incident reports. Tailored reports are agreed with the NECS Governance Team.
## 8.0 Duties and Responsibilities

<table>
<thead>
<tr>
<th>The Council of Members</th>
<th>Have delegated responsibility to the governing body (GB) 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.</th>
</tr>
</thead>
</table>
| Accountable Officer   | Has overall responsibility for:  
- the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements;  
- ensuring the incident management process is robust and adhered too;  
- ensuring incidents are maintained and managed in a timely manner;  
- ensuring staff have the necessary training required to implement the policy;  
- ensuring mechanisms are in place within the organisation for regular reporting and monitoring of incident themes and lesson learnt. |
| Service leads         | The service leads have the responsibility to:  
- support staff to maintain the incident policy and to manage individual incidents in accordance with policy;  
- work closely with the accountable officer to ensure a transparent and consistent approach to incident management across the CCG in partnership with key stakeholders. |
| Information Governance Lead | The CCG Information Governance Lead has the responsibility:  
- to provide information governance support to staff in the organisation;  
- to co-ordinate different areas of information governance and to ensure progress against key standards and requirements;  
- in collaboration with IT, develop, implement and monitor information security across the organisation  
- support the CCG in evidence collation, upload and publicise the IG Toolkit. |
<table>
<thead>
<tr>
<th><strong>All Staff</strong></th>
<th>All staff, including temporary and agency staff, are responsible for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• compliance with relevant process documents. Failure to comply may result in disciplinary action being taken;</td>
</tr>
<tr>
<td></td>
<td>• co-operating with the development and implementation of policies and procedures as part of their normal</td>
</tr>
<tr>
<td></td>
<td>• duties and responsibilities;</td>
</tr>
<tr>
<td></td>
<td>• identify the need for a change in policy or procedure as a result of becoming aware of changes to statutory</td>
</tr>
<tr>
<td></td>
<td>• requirements, revised professional or clinical standards and local/national directives, and advising their line</td>
</tr>
<tr>
<td></td>
<td>• manager;</td>
</tr>
<tr>
<td></td>
<td>• Attending training/awareness sessions when provided.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CSU</strong></th>
<th>Senior Governance Manager will:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• provide incident management support and advice</td>
</tr>
<tr>
<td></td>
<td>• produce CCG incident reports as requested;</td>
</tr>
<tr>
<td></td>
<td>• identify trends, lesson learned and themes in incident</td>
</tr>
<tr>
<td></td>
<td>• reporting in order to identify any issues of concern for</td>
</tr>
<tr>
<td></td>
<td>• the CCG;</td>
</tr>
<tr>
<td></td>
<td>• provide training and assistance to the CCG in incident</td>
</tr>
<tr>
<td></td>
<td>• reporting and management in the SIRMS system;</td>
</tr>
<tr>
<td></td>
<td>• manage the administration of the SIRMS database;</td>
</tr>
<tr>
<td></td>
<td>• undertake an incident investigation in conjunction with</td>
</tr>
<tr>
<td></td>
<td>• CCG managers if required e.g. health and safety and IG</td>
</tr>
<tr>
<td></td>
<td>• incidents.</td>
</tr>
</tbody>
</table>

The CSU Clinical Quality Manager will consider if a serious incident falls into the category of a STEIS reportable SI and report accordingly. Review clinical quality incidents reported by the CCG.

Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures

### 9.0 Implementation

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

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

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 CCG, NECS and their Member Practices.

This policy is reviewed at regular intervals to ensure that the implementation of the processes contained in the policy is in line with the practical experience of users of the SIRMS system.
10.0 Training Implications

The level of training required in incident reporting and management varies depending on the level and responsibility of the individual employee. These training requirements for the relevant staff groups in summary are:

<table>
<thead>
<tr>
<th>Training</th>
<th>Staff Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>General training / awareness in the use of the Safeguard incident reporting web-form</td>
<td>All staff</td>
</tr>
<tr>
<td>SIRMS incident reporting web-form for managers</td>
<td>Managers</td>
</tr>
<tr>
<td>SIRMS database training</td>
<td>SIRMS staff and specialist managers</td>
</tr>
<tr>
<td>Root Cause Analysis and incident investigation</td>
<td>Senior managers.</td>
</tr>
</tbody>
</table>

The sponsoring directors will ensure that the necessary training or education needs and methods required to implement the framework/procedure(s) 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.

11.0 Fair Blame

The CCG 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;
- 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.

11.1 Support for staff, and others
When an incident is reported it can be a stressful time for anyone involved, whether they are members of staff, a patient directly involved or a witness to the incident. They all need to know that they are going to be treated fairly and that lessons will be learnt and action taken to prevent the incident happening again.

During an incident investigation, appropriate support will be offered to staff and anyone else involved in the incident if required. Support includes access to counselling services and the provision of regular updates of the investigation and its outcomes. Information is available on request from the Governance Team.

12.0 Documentation

12.1 Other CCG Related Documents

CCG CO13 Risk Management: Policy and Procedure;
CCG CO06 Anti-Fraud Policy;
CCG CO07 Health & Safety: Policy & Corporate Procedures;
CCG CO18 Policy and Procedure Guidance for Reporting and Management of Serious Incidents (SIs);
POL Business Continuity Plan.

12.2 NHS policy, legislation and statutory requirements

The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (HMSO) 1995;

NHS England Draft Policy and Guidance for reporting and management of Serious Untoward Incidents, October 2007;

Working together to safeguard children, HM Government 2006;

No secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse (Department of Health 2000);

NHS England Incident Reporting Policy October 2012;

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation February 2015";

IG Incident Reporting Tool User Guide.

12.3 References

The major references consulted in preparing this policy are described above.
13.0 Monitoring, Review and Archiving

13.1 Monitoring

The CCG Corporate Governance & Risk Officer will agree with the Chief Finance Officer a method for the monitoring, dissemination and implementation of this framework.

13.2 Review

The 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.**

Staff who become aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives that affect, or could potentially affect policy documents, should advise the Corporate Governance and Risk Officer who, with the Chief Finance Officer, will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

13.3 Archiving

The Executive Group will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: NHS Code of Practice 2006.
### 14. Equality Analysis

**Equality Analysis Screening Template (Abridged)**

<table>
<thead>
<tr>
<th>Title of Policy:</th>
<th>Incident Reporting &amp; Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short description of Policy (e.g. aims and objectives):</td>
<td>This policy sets out the CCG’s approach to the management of incidents in fulfilment of its strategic objectives and statutory obligations. The reporting of incidents will help the CCG identify potential breaches in its core business including breaches in:</td>
</tr>
<tr>
<td></td>
<td>• contractual obligations;</td>
</tr>
<tr>
<td></td>
<td>• internal processes;</td>
</tr>
<tr>
<td></td>
<td>• performance targets;</td>
</tr>
<tr>
<td></td>
<td>• service specifications etc.;</td>
</tr>
<tr>
<td></td>
<td>• Statutory duties.</td>
</tr>
</tbody>
</table>

**Directorate Lead:** Chief Finance Office

**Is this a new or existing policy?** Existing

**Equality Group**

<table>
<thead>
<tr>
<th>Age</th>
<th>Neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disability</td>
<td>Neutral</td>
</tr>
<tr>
<td>Gender Reassignment</td>
<td>Neutral</td>
</tr>
<tr>
<td>Marriage And Civil Partnership</td>
<td>Neutral</td>
</tr>
<tr>
<td>Pregnancy And Maternity</td>
<td>Neutral</td>
</tr>
<tr>
<td>Race</td>
<td>Neutral</td>
</tr>
<tr>
<td>Religion Or Belief</td>
<td>Neutral</td>
</tr>
<tr>
<td>Sex</td>
<td>Neutral</td>
</tr>
<tr>
<td>Sexual Orientation</td>
<td>Neutral</td>
</tr>
<tr>
<td>Carers</td>
<td>Neutral</td>
</tr>
</tbody>
</table>

**Does this policy have a positive, neutral or negative impact on any of the equality groups?** Please state which for each group.

**Screening Completed By**

<table>
<thead>
<tr>
<th>Julie Rutherford</th>
<th>Job Title and Directorate</th>
<th>Organisation</th>
<th>Date completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Officer</td>
<td>Governance</td>
<td>NECS</td>
<td>9/02/2015</td>
</tr>
</tbody>
</table>

**Directors Name**

<table>
<thead>
<tr>
<th>Simon Gregory</th>
<th>Directors Signature</th>
<th>Organisation</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>South Tees CCG</td>
<td>13/05/15</td>
</tr>
</tbody>
</table>
Appendix 1

Glossary of Terms

The following terms are used in this document:

**A Business Continuity Incident**
An unwanted event that threatens personnel, buildings, operational procedures or the reputation of the organisation which requires special measures to be taken to restore things back to normal.

**Corporate Business Incidents**
A corporate business incident is an event or circumstance that could have or did have a negative impact on the way the CCG does business with stakeholders and that could lead to financial loss.

**Clinical Incidents**
A clinical incident is any unintended or unexpected incident which could have or did lead to harm for one or more patients receiving NHS care.

**Cyber Incident**
A Cyber-related incident 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 our businesses, infrastructure and services.” Source: UK Cyber Security Strategy, 2011

Types of incidents could include:

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

**Fraud and Corruption**

Fraud is essentially dishonest behavior and is in very simple terms, “stealing”. An NHS insider may claim money for services not provided, claim more money than they are entitled to, or divert funds to themselves in other ways. External organisations may provide false or misleading information, for example through invoices, to claim money they are not entitled to.
Harm
Harm is defined as an ‘injury (physical or psychological), disease, suffering disability or death’. In most circumstances harm can be considered to be unexpected, rather than the natural cause of the patient’s underlying condition.

Health and Safety, Fire, Environmental and Security Incidents
A health and safety, fire, environmental or security incident is an event or circumstance that affects staff/visitors safety. A reportable health and safety incident will fall under one of the following categories:

- **estates facilities** - could include a water leak, a lack of electricity occurring in buildings;
- **environmental** – impact on land, air or watercourses;
- **fire** - could include fire outbreak, false alarm;
- **health and safety other** – not falling in to any of the above categories;
- **staff ill health** - could include seizures, work related disorders;
- **security** - could involve damage, loss, theft;
- **staff accident** – e.g. slips, trips and falls, injuries to persons.

Information Governance Incidents
An information governance incident is an event or circumstance which could, or does, negatively affect the security of the information maintained by the CCG.

IG incidents will fall in to one of the following cause groups:

- damage to hard copy records;
- inappropriate access to/or disclosure of a person’s information;
- information left unattended (printer, empty office);
- lost/stolen – equipment;
- misdirected email containing confidential information;
- misdirected hardcopy (e.g. post, fax etc.);
- password/smartcard sharing.

Information Technology (IT) Incidents –
An information technology (I.T.) incident is an event or circumstance that affects or could affect the way the CCG does business negatively and is attributed to I.T. systems and/or the network. These incidents will most often include, but are not limited to:

- hardware failure;
- network failure;
- software failure;
- server failure;
- telecommunications failure;
- virus discovery.

Near Miss
An incident could be a **near miss** which is an event or situation that has the potential to cause harm but which never happened. These events should also be reported so the organisation can learn lessons and take preventative action where required.
NRLS (The National Reporting and Learning System)

The NRLS is a central database of [patient safety incident reports](#). Since the NRLS was set up in 2003, over four million incident reports have been submitted.

All information submitted is analysed to identify hazards, risks and opportunities to continuously improve the safety of patient care.

RCA (Root Cause Analysis)

RCA is a systematic process whereby the factors that contributed to an incident are identified. As an investigation technique for incidents, it looks beyond the individuals concerned and seeks to understand the underlying causes and environmental context in which an incident happened.

Serious Incidents

“A serious incident is an incident related to NHS-funded services and care resulting in one of the following:

- unexpected or avoidable death of one or more patients, staff, visitors or members of the public;
- serious harm to one or more patients, staff, visitors or members of the public or where the outcome requires life-saving intervention, major surgical/medical intervention, permanent harm or will shorten life expectancy or result in prolonged pain or psychological harm (this includes incidents graded under the NPSA definition of severe harm);
- a scenario that prevents or threatens to prevent a provider organisation’s ability to continue to deliver healthcare services, for example, actual or potential loss of personal/organisational information, damage to property, reputation or the environment, IT failure or incidents in population programmes like screening and immunisation where harm potentially may extend to a large population;
- allegations of abuse;
- adverse media coverage or public concern about the organisation or the wider NHS;
- one of the core set of never events.”

This is a serious incident requiring investigation. Incidents falling into this category are essentially information governance or IT security related. These incidents must be reported to the DH (Department of Health) and the ICO (Information Commission Office) via the Health and Social Care Information Centre Information Governance Toolkit. Where it is suspected that an IG SIRI has taken place, it is good practice to informally notify key staff (Chief Executive, SIRO, Caldicott Guardian, other Directors etc.) as an ‘early warning’ to ensure that they are in a position to respond to enquiries from third parties and to avoid ‘surprises’. For cyber incidents notify the person responsible for any operational response (typically the Head of IT).
Soft Intelligence

Information gathered about a provider and its services, either from those who have experienced that service or from those with a professional relationship with the service. There may not be substantiated evidence to prove whether or not the event or experience occurred or has had an immediate measurable impact, but the intelligence may contribute to the bigger picture when looked at alongside hard intelligence and other evidence based information.

The Strategic Executive Information System (STEIS)

STEIS is a national database for reporting and learning from the most serious incidents in the NHS.

The CSU Clinical Quality Team is responsible for recording serious incidents onto STEIS. This system is to be replaced by a new national consolidated system for reporting and learning from serious incidents in the near future.
Appendix 2

How to report an incident on SIRMS guide

Incident Reporting Form

Please enter details of the incident that has occurred. All incidents should be entered using this form. Should you have any questions please contact the NECU Corporate Governance or Clinical Quality Teams at your local NECU office.

Details of Person completing this form

- Your details will automatically be filled in, if there are any errors, please contact necu.sirmsemail@nhs.net

- This section forms part of the notification that this is sent to your manager and/or specialists so that they can investigate the incident, therefore it is important not to include sensitive information such as names.

- Yellow fields are mandatory

- Type of incident can be clinical, non-clinical, soft intelligence or a 111 incident

- Primary cause groups are categories of incidents, choosing 1 of these from the drop down options will affect the cause choices in the next field. If you're unable to find appropriate cause, try selecting a different cause group.

- Selecting 'yes' on any of these fields will open up further sections that should be completed.

- Use this section to provide details of any action taken immediately after the incident took place.
Appendix 3

How managers should manage incidents on SIRMs guide

The first sections contain the details of the incident report that was submitted. These sections are read only, except where specifically highlighted (see below).

Managers should check the information has been given.

If anything important has been omitted or if the ‘details’ contains Personal Identifiable Data, return to the reporter. (This can be done from the front page of the incident management section – click on ‘Notifications’ tab.)

If a member of staff is absent from work for 7+ days it must be reported to the HSE under RIDDOR.

The NECS Senior Governance Officer (H&S) will submit the RIDDOR report.

These sections continue the incident report that was submitted.

Managers should check the information and add more details if necessary.

If the incident involves a patient, the details can only be entered by the incident manager. Only incidents with an Actual Impact grading of 4 or 5 should include patient details.

See ‘SIRMS Actual Impact SOP’ for more information.
The investigation of an incident may highlight what caused it to happen, such as not following correct policy or procedure, human error, etc. or may identify a training need, a resource requirement etc. Managers should provide details here.

Provide a summary of what actions have been taken to rectify the incident.

It is important that managers reflect on what has gone wrong. In particular, an incident might highlight system failures which need to be corrected. Learning from incidents can be shared, if appropriate, with other team members, wider directorate or across the whole organisation.

It's good practice to feedback to the reporter details of the investigation and any remedial actions or planned actions. The system can send an email to the reporter, click ‘Yes’ to do this.

If there are relevant documents that would help with the investigation, upload them here. Click ‘Add’ and you will then be able to upload from network files.

If you have not completed the form, you can’t save and continue’, but it is important to report incidents as soon as possible.

Once you are sure the form is complete, ‘save and close’. A notification of the incident will be sent to relevant managers.
Process for managing corporate business incidents flowchart

South Tees CCG Corporate Business Incident Management Process

A corporate business incident is a business event or circumstance that could have or did have a negative impact on its internal/external stakeholders. The impact of the incident would have a negative impact on quality and service delivery. A corporate business incident that is reportable is likely to include one or more of the following:

- A lack of capacity or a service gap in meeting our commissioning responsibilities;
- A quality concern;
- A communications breakdown.

1. **Recording a Corporate Business Incident**

   All CCG staff (permanent, fixed term and contractors) have a duty to report the incidents that they are involved in or witness. Staff are instructed to use the CCG/GP incident reporting page on SIRMS to report these incidents. SIRMS can be accessed via the following link [https://sirms.necsu.nhs.uk](https://sirms.necsu.nhs.uk). When recording the incident on SIRMS you will be asked to score the incident. Refer to appendix 8 incident risk matrix.

2. **Is the incident Serious?**

   Any incident with an incident score of 5 (catastrophic) or 4 (major) will be referred immediately to the Chief Finance Officer, Chief Officer and to the CSU Specialist Officer (the designated CRM). An immediate management response is required and a route cause analysis must be carried out. Refer to appendix 10 route cause analysis guide.

3. **Corporate Business Incidents score 1-3**

   Those incidents with a score of 1-3 on the incident risk matrix are not classed as serious but still must be checked within 24 hours on SIRMS. The Corporate Risk and Governance Officer will be notified of the incident via SIRMS and will sign post the incident to a CCG Investigating Incident Manager who will be responsible for its management.

4. **Managing an incident on SIRMS**

   All incidents must be managed on SIRMS. The Investigating Incident Manager must consider if it is necessary to carry out a route cause analysis of the incident. Refer to appendix 10 route cause analysis guide.

   The Investigating Incident Manager will provide feedback to the reporter of the incident.
5. Timeline for managing and closing incidents
Managers will have allocated a colour coded impact rating when managing their incidents on SIRMS. The colour indicates the timeline for managing the incident and the process for closing the incident down.

<table>
<thead>
<tr>
<th></th>
<th>Negligible/no harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incident to be noted and closed off within 5 days.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Low risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Incident Investigating Manager to manage and close off the incident within 5 days.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Medium risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>The Incident Investigating Manager will manage and close off the incident within 5 days.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>High risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Once recorded these incident must be referred immediately to the Chief Finance Officer, Chief Officer and the CSU Specialist Officer. A management response is required as soon as possible within a 24 hour period. The Chief Finance Officer to close off the incident within 1 month. If the close off target is not met an interim report of progress needs to be submitted to the Corporate Risk and Governance Officer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Once recorded these incident must be referred immediately to the Chief Finance Officer, Chief Officer and a CSU Specialist Officer. A management response is required as soon as possible within a 24 hour period. The Chief Finance Officer to close off the incident within 1 month. (If the close off target is not met an interim report of progress needs to be submitted to the Corporate Risk and Governance Officer.</td>
</tr>
</tbody>
</table>

6. CSU Governance Team will finally close and archive the incident on SIRMS
Once Governance and Risk Committee has reviewed the incident and agreed recommendations and remedial actions are in place, the incident will be closed and archived on SIRMS by the Governance Team.

7. Incident Themes and Trends and Learning Lessons
An overview of incidents reported across the organisation will be monitored quarterly for trends, themes and lessons learnt at Governance and Risk Committee.
**List Specialist Officers (do we use telephone numbers or email addresses)**

CSU/NECS Corporate Business named contact customer leads for incidents (tailor to CCG)

- Cumbria CCG - **Joanne Dobson**: joannedobson@nhs.net - 07771345502
- Durham - (Darlington, North Durham & DDES CCGs) & South Tees CCG - **Mike Brierley**: mike.brierley@nhs.net 07971905867
- Newburn (Newcastle East, Newcastle West, Gateshead Alliance CCGs) & HaST CCG - **Khalid Azam**: khalid.azam@nhs.net 07788566828
- Newburn (Sunderland, South Tyneside, North Tyneside, Northumberland CCGs) - **Ailsa Nokes**: ailsa.nokes@nhs.net 07826532501

SIRMS queries can be made to the NECS Governance Team:-
NECSU.SIRMSINCIDENTS@nhs.net
Appendix 5

Process for managing health and safety incidents flowchart

South Tees CCG Health and Safety Incident Management Process

A health and safety, fire, environmental or security incident is an event or circumstance that affects staff/visitors safety.

A reportable health and safety incidents will fall under one of the following categories:

- **Estates facilities** - could include a water leak, a lack of electricity occurring in NECS buildings;
- **Environmental** – impact on land, air or watercourses;
- **Fire** - could include fire outbreak, false alarm;
- **Health and safety other** – not falling in to any of the above categories;
- **Staff ill health** - could include seizures, work related disorders;
- **Security** - could involve damage, loss, theft;
- **Staff accident** – e.g. slips, trips and falls, injuries to persons.

1. **Recording a Health and Safety Incident**

All CCG staff (permanent, fixed term and contractors) have a duty to report an incident they are involved in or witness.

Staff are instructed to use the CCG/GP reported incident reporting page on SIRMS to report these incidents. SIRMS can be accessed via the following link:

https://sirms.necsu.nhs.uk. When recording the incident on SIRMS you will be asked to score the incident. Refer to the CCG incident risk matrix at appendix 8.

Any Incidents relating to defects or issues within the building MUST be reported to the relevant NHS Property Services/Local Authority Help Desk immediately details of which can be obtained from the NECS Health and Safety Team

necsu.healthandsafety@nhs.net

2. **Is the Incident Serious?**

Any incident with a consequence score of 5 (catastrophic) or 4 (major) is classed as serious and will be referred immediately to the Chief Finance Officer, Chief Officer and the CSU Health and Safety Officer.

If the incident is confirmed to be serious, the H&S serious incident procedure will be invoked immediately and a route cause analysis must be carried out.

**Note**

The CCG is statutory obliged to report RIDDOR (Report of Injuries, Diseases and Dangerous occurrences REGS, 1995) incidents to the Health and Safety Executive. Incidents must be reported to RIDDOR when someone has been absent from work for more than 7 days Your Health and Safety Specialist will report the incident to the H&S Exec on the CCGS behalf. If the incident recorded falls in to this category please email your health and safety specialist on necsu.healthandsafety@nhs.net and advise accordingly.
3. Health and Safety Incidents with a score of 1-3

Those incidents with a score of 1-3 on the incident matrix are not classed as serious but must still be checked within 24 hours on SIRMS. The Corporate Risk and Governance Officer will be notified of the incident via SIRMS and will sign post the incident to a CCG Incident Investigating Manager, who will be responsible for management of the incident.

4. Managing the incident on SIRMS

All incidents should be managed on SIRMS. The Incident Investigating Manager must consider if it is necessary to carry out a route cause analysis of the incident.

The Investigating Incident Manager will provide feedback to the reporter.

5. Timeline for managing and closing incidents

Managers will have allocated a colour coded impact rating when managing their incidents on SIRMS. The colour indicates the timeline for managing the incident and process for closing the incident down.

<table>
<thead>
<tr>
<th></th>
<th>Impact Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Negligible/no harm</td>
<td>Incident to be noted and closed off within 5 days.</td>
</tr>
<tr>
<td>2</td>
<td>Low risk</td>
<td>The CCG Incident Investigating Manager will manage and close off the incident within 5 days.</td>
</tr>
<tr>
<td>3</td>
<td>Medium risk</td>
<td>The Incident Investigating Manager will manage and close off the incident within 5 days.</td>
</tr>
<tr>
<td>4</td>
<td>High risk</td>
<td>Once recorded these incidents must be referred immediately to the Chief Finance Officer, Chief Officer and a CSU Specialist Officer. A management response is required as soon as possible within a 24 hours period. The Chief Finance Officer will close off the incident within 1 month. If the close off target is not met an interim report of progress should be submitted to the Corporate Risk and Governance Officer.</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Once recorded these incident must be referred immediately to the Chief Finance Officer, Chief Officer and the CSU Specialist Officer. A management response is required as soon as possible within a 24 hour period. The Chief Finance Officer must manage and close off the incident within 1 month. If the close off target is not met an interim report of progress must be submitted to the Corporate Risk and Governance Officer.</td>
</tr>
</tbody>
</table>
6. NECS Governance Team will finally close and archive the incident on SIRMS

Once the Governance and Risk Committee has reviewed the incident and agreed recommendations and remedial actions are in place, the incident will be closed and archived on SIRMS.

7. Monitoring Themes, Trends and Lessons Learnt

An overview of incidents reported across the organisation will be monitored for trends, themes and lessons learnt through the Governance and Risk Committee.

Useful Contacts

- CCG Corporate Risk and Governance Officer
- NECS H&S Contact – necsu.healthandsafety@nhs.net
- CCG Incident Process - NECSU.SIRMSINCIDENTS@nhs.net
- SIRMS queries - NECSU.SIRMSINCIDENTS@nhs.net
Information Governance (IG) Incidents

An information governance incident is an event or circumstance which affects or could affect the security of the information maintained by the CCG.

IG incidents will fall in to one of the following cause groups:

- damage to hard copy records;
- inappropriate access to/or disclosure of a person’s information;
- information left unattended (printer, empty office);
- lost/stolen – equipment;
- misdirected email containing confidential information;
- misdirected hardcopy (e.g. post, fax etc.);
- password sharing/smart card sharing;
- IT Network failure.
- cyber incident

1. Recording an IG/IT Incident

All CCG staff (permanent, fixed term and contractors) have a duty to report IG/IT incidents that they are involved in or witness. Staff are instructed to use the CCG/GP incident reporting page on SIRMS to report these incidents. SIRMS can be accessed via the following link: https://sirms.necsu.nhs.uk. When recording the incident on SIRMS you will be asked to score the incident. Refer to the CCG Incident matrix at appendix 5.

2. Is the Incident Serious?

Any incident with a score of 5 (catastrophic) or 4 (major) will be referred immediately to the Chief Officer, SIRO, Caldecott Guardian and Corporate Governance and Risk Officer. The CSU Senior Governance Manager for Information Governance and Head of Communications should also be notified. An immediate management response is required and a route cause analysis should be carried out.

Please note:

3. IG Incidents scored 1-3 on the incident matrix:

Those incidents with a score of 1 -3 on the incident matrix are not classed as serious but these should still be checked in a 24 hour period on SIRMS. The Corporate Risk and Governance Officer will be notified of the incident via SIRMS and will sign post the incident to a CCG Incident Investigating Manager, who will be responsible for management of the incident.

From June 2013 all Organisations processing health and adult social care personal data were required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the DH, ICO and other regulators.

There is no simple definition for an IG serious incident requiring investigation (SIRI). With an IG or IT Security incident what first appears to be of minor importance may, on further investigation be found to be serious, and vice versa. It is because of this that all IG incidents reported on SIRMS will be quality checked daily by the NECS Information Governance Team to assess if the incident needs to be reported to the Department of Health Information Commissioner via the IG Toolkit.

If the incident is found to be serious NECS Information Governance Team will also refer the incident to NECS Clinical Quality Team who has the responsibility of reporting serious incidents to the NPSA (National Patient Safety Agency). NPSA will record the incident on the Serious Incident Reporting and Learning Framework (SIRL) via STEIS.
### 4. Managing an incident on SIRMS

All incidents should be managed on SIRMS.

The incident investigating manager must consider if it is necessary to carry out a route cause analysis of the incident.

### 5. Timeline for managing and closing incidents

Managers will have allocated a colour coded impact rating when managing their incidents on SIRMS. The colour indicates the timeline for managing the incident and the process for closing the incident down.

<table>
<thead>
<tr>
<th></th>
<th>Negligible/no harm</th>
<th>Low risk</th>
<th>Medium risk</th>
<th>High risk</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incident to be noted and closed off within 5 days.</td>
<td>The CCG Incident Investigating Manager will manage and close off the incident within 5 days.</td>
<td>The Incident Investigating Manager will manage and close off the incident within 5 days.</td>
<td>High risk Catastrophic – Once recorded these incident must be referred immediately to the Chief Officer, SIRO, Caldicott Guardian and Corporate Governance and Risk Officer and the CSU IG Lead. A management response is required as soon as possible within 24 hour period. The Chief Officer should close off the incident within 2 days. If the close off target is not met an interim report of progress needs to be submitted to the Corporate Risk and Governance Officer.</td>
<td>Catastrophic – Once recorded these incident must be referred immediately to the Chief Officer, SIRO, Caldecott Guardian and Corporate Governance and Risk Officer and the CSU IG Lead. A management response is required as soon as possible within a 24 hour period. The Chief Officer must manage and close off the incident within 2 days. (If the close off target is not met an interim report of progress must be submitted to the Risk and Governance Officer).</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 6. NECS Governance Team will finally close and archive the incident on SIRMS

Once Risk and Governance Committee has reviewed the incident and agreed recommendations and remedial actions are in place, the incident will be closed and archived on SIRMS.

### 7. Monitoring Themes, Trends and Lessons Learnt

An overview of incidents reported across the organisation will be monitored for trends, themes and lessons learnt through the Risk and Governance Committee.
For further information or help please contact one of the following:

- CCG IG Lead
- CCG Risk and Governance Officer
- CSU IG/IT specialist
- SIRMS query – email address NECSU.SIRMSINCIDENTS@nhs.net
Appendix 7

Process for managing NECS clinical incidents flowchart

CCG Clinical Quality Incident Management Process

1. **Record the Incident**

Clinical Quality incidents can be recorded by CCG staff when they become aware of service quality, delivery or contracting issue in one of their commissioned providers. Along with similar intelligence recorded by the CCG Member Practices, these incidents can help identify areas for improvement in quality, performance and commissioning.

All staff (permanent, fixed term and contractors) should report any clinical quality incidents they are aware of. To report these staff should use the **CCG/GP reporting an incident** page of SIRMS which can be accessed via the following link [https://sirms.necsu.nhs.uk](https://sirms.necsu.nhs.uk)

2. **Determine if the Clinical Quality Incident is a Serious Incident**

The NECS clinical quality team monitor and review all clinical quality incidents to determine the likely impact score of the incident.

An incident with a score of 4 to 5 on the incident impact assessment scale will be further assessed to determine whether it meets the national guidance criteria as a reportable **Serious Incident** which will require external reporting on the STeIS system. **Serious Incidents** are outlined in the [national guidance](https://) and the CCG Serious Incident policy and can be clinical or non-clinical in nature.

The NECS Clinical Quality Team will liaise with the CCG quality and/or governance lead to report the serious incident onto STeIS on behalf of the CCG where the alleged incident has occurred. The CCG Manager and the NECS Clinical Quality Team will then agree if the CCG serious incident procedure needs to be invoked.

3. **Managing a Clinical Quality Incident on SIRMS**

All clinical quality incidents reported on SIRMS will be managed by the clinical quality team covering the CCG area from which the incident was reported. CQ will manage the incident on **SIRMS via the SIRMS Managers form and will**:

I. Review the content and quality of the information entered to ensure the correct incident categories etc. have been completed;

II. Assess the impact of the incident and score it accordingly;
  - 1-3, 6&7: Identify any themes and trends across similar incident types and share incident at regular monthly meetings with Providers in thematic reports;
  - 4-5: Request NHS Number or other patient identifiable data from reporter (if relevant) and request individual investigation carried out within 2 weeks.
  - Provide feedback to the reporter on actions taken on the incident.
4. **Advise the reporter**
The NECS Clinical Quality Team will provide feedback to the reporter and will:

1. Thank the reporter for reporting the issue;
2. Provide a description of any changes made to form and why they were made;
3. Request that they or their manager complete the sections on Actions, Root Causes and Outcomes where relevant;
4. Provide a brief description of what will happen with the incident (e.g. included in themes & trend or specific response requested from Trust etc.)

5. **Timeline for managing and closing clinical quality incidents**

Reporters will have allocated a colour coded impact rating when reporting their incidents on SIRMS. The RAG rating gives a recommended indication of the timeline for managing the incident and the expected action for management. Managers can review this rating based on their understanding of the incident.

<table>
<thead>
<tr>
<th></th>
<th>Negligible/no harm</th>
<th>Low risk</th>
<th>Medium risk</th>
<th>High risk</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incident to be noted and closed off within 5 days</td>
<td>Manager to review incident within 5 working days and share with Provider in monthly reports. Incident themes and trends to be shared at internal CCG quality group and Provider QRG.</td>
<td>Manager to review incident within 5 working days and share with Provider in monthly reports. Incident themes and trends to be shared at internal CCG quality group and Provider QRG.</td>
<td>The incident should be reviewed as soon as possible, ideally within 48 hours, of reporting. CCG Head of Quality &amp; Safety (or equivalent) will work with the CQ team to request an initial response from the provider within 2 weeks and a subsequent full response within 4 weeks. All incidents of this grade will be monitored through the internal CCG quality group and Provider QRG. Closure of the incident will be finally ratified by the CCG internal quality group.</td>
<td>Once recorded these incidents should be referred immediately to the CCG Head of Quality &amp; Safety (or equivalent) and the NECS Senior Clinical Quality Programme Lead. Initial review and response is required as soon as possible within a 24 hour period. CCG Head of Quality &amp; Safety (or equivalent) will work with the CQ team to request an initial response from the provider within 2 weeks and a subsequent full response within 4 weeks. All incidents of this grade will be monitored through the internal CCG quality group and Provider QRG. Closure of the incident will be finally ratified by the CCG internal quality group.</td>
</tr>
<tr>
<td>2,6,7</td>
<td>Low risk</td>
<td>Manag</td>
<td>Manager to review incident within 5 working days and share with Provider in monthly reports. Incident themes and trends to be shared at internal CCG quality group and Provider QRG.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Medium risk</td>
<td>Manager to review incident within 5 working days and share with Provider in monthly reports. Incident themes and trends to be shared at internal CCG quality group and Provider QRG.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>High risk</td>
<td>The incident should be reviewed as soon as possible, ideally within 48 hours, of reporting. CCG Head of Quality &amp; Safety (or equivalent) will work with the CQ team to request an initial response from the provider within 2 weeks and a subsequent full response within 4 weeks. All incidents of this grade will be monitored through the internal CCG quality group and Provider QRG. Closure of the incident will be finally ratified by the CCG internal quality group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Once recorded these incidents should be referred immediately to the CCG Head of Quality &amp; Safety (or equivalent) and the NECS Senior Clinical Quality Programme Lead. Initial review and response is required as soon as possible within a 24 hour period. CCG Head of Quality &amp; Safety (or equivalent) will work with the CQ team to request an initial response from the provider within 2 weeks and a subsequent full response within 4 weeks. All incidents of this grade will be monitored through the internal CCG quality group and Provider QRG. Closure of the incident will be finally ratified by the CCG internal quality group.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. **NECS Clinical Quality Team will close the incident on SIRMS**

Once recommendations and remedial actions are in place and the incident has been closed down by the internal CCG Quality Group. A summary of incident themes, trends and outcomes will be provided in the regular clinical quality reports to the CCG
For further information please email

<table>
<thead>
<tr>
<th>Specialist Contacts</th>
<th>Area</th>
<th>Emails Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kirstie Hesketh – Senior Manager Clinical Quality</td>
<td>Clinical Incidents</td>
<td><a href="mailto:necsu.incidents@nhs.net">necsu.incidents@nhs.net</a></td>
</tr>
<tr>
<td>Daniel Webber – Clinical Quality Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Julie Rutherford Governance</td>
<td>SIRMS queries -</td>
<td><a href="mailto:NECSU.SIRMSINCIDENTS@nhs.net">NECSU.SIRMSINCIDENTS@nhs.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 8

Incident Risk Matrix

CCG Incident Assessment Matrix

Introduction

A risk-based approach is used to link incidents to the risk management framework.

The use of an incident grading system will help to assess the level of risk attributed to an incident, its seriousness and the level of investigation or analysis to be undertaken.

In some cases the outcome of the incident is such that it is immediately obvious that the incident is serious or significant.

When assessing the risk of an incident, reporters should use the risk matrix outlined below.

Assessing the Incident

Step 1: Determine the consequence score of your incident

From the submitted incident make a note of the cause group and use the corresponding table below to assess the consequence rating, the number is given at the top of the column.

The consequence score will either be:

- Negligible,
- Minor,
- Moderate,
- Major
- Or catastrophic.

When scoring the consequence you are assessing either:

- The consequence of the incident that has occurred
- Or the likely consequence of a near miss should the incident have occurred

NOTE

Any incident with a consequence score of 5 (catastrophic) or 4 (major) needs to be referred immediately to the responsible Director and NECS Specialist Officer. An immediate management response is required. The incident needs to be recorded on SIRMS. Once recorded on SIRMS the above contacts will be notified automatically.

Incident Scoring Matrix
## Consequence score (severity levels) and examples of descriptors

<table>
<thead>
<tr>
<th>Domains</th>
<th>1 (Negligible/no Harm)</th>
<th>2 (Minor)</th>
<th>3 (Moderate)</th>
<th>4 Serious</th>
<th>5 Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmenta l incident Impacting on (air, land, water, waste management,) (includes building security and fire)</td>
<td>Loss/interruption of &gt;1 hourrees/time/minimal impact on the environment / Nuisance release</td>
<td>Loss/interruption of &gt;8 hours Minor impact on environment Onsite impact contained by organisation</td>
<td>Loss/interruption of &gt;1 day Moderate impact on environment On-site impact contained by organisation</td>
<td>Loss/interruption of &gt;1 week Major impact on environment External assistance required e.g. NHS Property Services</td>
<td>Permanent loss of service or facility Catastrophic impact on environment Off-site impact requiring outside assistance</td>
</tr>
<tr>
<td>Impact on the safety of patients, staff or public (physical/psychological harm)</td>
<td>Minimal injury requiring no/minimal intervention or treatment. No time off work</td>
<td>Minor injury or illness, requiring minor intervention Short-term injury requiring time off for &gt;3 days Length of hospital stay by 1-3 days Emotional distress recovery expected within day</td>
<td>Moderate injury requiring professional intervention Requiring time off work for 4-14 days Length of hospital stay by 4-15 days</td>
<td>Serious Incident Major injury leading to long-term incapacity/disability/emotional trauma Requiring time off work for &gt;14 days Increase in length of hospital stay by &gt;15 days</td>
<td>Serious Incident leading to one or more deaths Multiple permanent injuries or irreversible health effects</td>
</tr>
</tbody>
</table>

This also includes individual security i.e. loan working
## Consequence score (severity levels) and examples of descriptors

<table>
<thead>
<tr>
<th>Domains</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4 Serious</th>
<th>5 Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adverse publicity/reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rumours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential for public concern</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local media coverage – short-term reduction in public confidence</td>
<td>Negligible</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Elements of public expectation not being met</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National media coverage with &lt;3 days service well below reasonable public expectation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National media coverage with &gt;3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate Business Incidents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer impact little to none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of Contract none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial impact negligible £</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occurrence multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of customers affected one</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statutory compliance not breached</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate Customer impact little to none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of Contract none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial impact £10k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occurrence multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of services affected one</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statutory compliance not breached</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer impact high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of contract none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial impact 10k-100k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occurrence multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of customers services affected multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statutory compliance not breached</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance SFI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer impact extreme</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of contract yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial impact £1 million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occurrence multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of customers services affected multiple</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statutory compliance not breached</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of OJE Procurement Regs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td>Negligible</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
<td>-------</td>
<td>----------</td>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>Finance including claims</td>
<td>Small loss</td>
<td>Loss of 0.1–0.25 per cent of budget</td>
<td>Loss of 0.25–0.5 per cent of budget</td>
<td>Uncertain delivery of key objective/Loss of &gt;1 per cent of budget</td>
<td>Non-delivery of key objective/Loss of &gt;1 per cent of budget</td>
</tr>
<tr>
<td></td>
<td>Risk of claim remote</td>
<td>Claim less than £10,000</td>
<td>Claim(s) between £10,000 and £100,000</td>
<td>Claim(s) between £100,000 and £1 million Purchasers failing to pay on time</td>
<td>Failure to meet specification/slippage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Loss of contract / payment by results</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Claim(s) &gt;£1 million</td>
</tr>
<tr>
<td>Information Governance</td>
<td>11-100 Serious potential breach of confidentiality</td>
<td>Breach of confidentiality e.g. up to 101 - 1000 people affected</td>
<td>Breach of confidentiality with particular sensitivity 1001 + people affected</td>
<td>Breach of confidentiality with particular sensitivity 2001 + people affected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.g. patient identifiable information at risk/clinical patient information at risk.</td>
<td>E.g. patient identifiable information at risk/clinical patient information at risk.</td>
<td>E.g. patient identifiable information at risk/clinical patient information at risk.</td>
<td>E.g. patient identifiable information at risk/clinical patient information at risk.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Or Failure to encrypt mobile data</td>
<td>Or Failure to encrypt mobile data</td>
<td>Newsworthy breach</td>
<td>Newsworthy breach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Or Failure to encrypt mobile data</td>
<td>Or Failure to encrypt mobile data</td>
<td>Or Failure to encrypt mobile data</td>
<td>Or Failure to encrypt mobile data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Newsworthy</td>
</tr>
</tbody>
</table>

E.g.:
- patient identifiable information at risk/clinical patient information at risk.
- Failure to encrypt mobile data
- News worthy
<table>
<thead>
<tr>
<th>Domains</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4 Serious</th>
<th>5 Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity</td>
<td>Negligible</td>
<td>Minor</td>
<td>Moderate</td>
<td>An unplanned interruption or reduction in the quality of a service to a small number of users</td>
<td>An interruption in service requiring immediate attention and affecting multiple customers at a site but not site wide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A non-standard service is down affecting multiple customers</td>
<td>A non-key service is down affecting multiple users and several locations</td>
<td>An interruption in service requiring immediate attention and affecting multiple customers at a site but not site wide</td>
<td>A partial loss of business critical systems or service including slow performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>An interruption in service requiring immediate attention. Affecting a whole site/service or the loss of a critical system/service</td>
<td>The interruption seriously affects NECS or our NECS customers organisational goals</td>
</tr>
<tr>
<td>NECS Clinical Quality Incidents</td>
<td>Peripheral element of treatment or service suboptimal</td>
<td>Overall treatment or service suboptimal</td>
<td>Treatment or service has significantly reduced effectiveness</td>
<td>Non-compliance with national standards with Major risk to patient safety if unresolved</td>
<td>Totally unacceptable level or quality of treatment/service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single failure to meet internal standards</td>
<td>Repeated failure to meet internal standards</td>
<td>Low performance rating</td>
<td>Gross failure, or potential failure, of patient safety if findings not acted on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor implications for patient safety if unresolved</td>
<td>Moderate patient safety implications if findings are not acted on</td>
<td>Critical report</td>
<td>Gross failure to meet national standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduced performance rating if unresolved</td>
<td></td>
<td>Major failure of provided service</td>
<td>Meets National Definition of a Serious Incident.</td>
</tr>
<tr>
<td>Consequence score (severity levels) and examples of descriptors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Domains</strong></td>
<td><strong>1 - Negligible</strong></td>
<td><strong>2 - Minor</strong></td>
<td><strong>3 - Moderate</strong></td>
<td><strong>4 - Serious</strong></td>
<td><strong>5 - Catastrophic</strong></td>
</tr>
<tr>
<td>IT incidents</td>
<td>Incidents involving non-standard service requests</td>
<td>Incidents involving Standard Service Requests re:</td>
<td>An unplanned interruption or reduction in the quality of an IT service to a small number of users. A non-key service is down affecting a multiple users in several locations.</td>
<td>An issue requiring immediate attention affecting multiple customers at a site but not site wide. A partial loss of a business critical system or service, including slow performance. One department or a team within a site unable to connect to a business critical services or system. A business critical service that has failed affecting a single user and no alternative is available.</td>
<td>An issue requiring immediate attention affecting a whole site/service of the loss of business critical system/service. The impact of the issue seriously affects organisational goals. An issue identified as a clinical risk, such as inaccurate patient records. Issue affects or threatens a key system or service. This could include</td>
</tr>
<tr>
<td></td>
<td>- A request from a user for a non-standard change</td>
<td>- Laptops</td>
<td>- Printer failure (excluding main officer script printers and IT those within dispensing practices where no alternative is available.)</td>
<td>- One department or a team within a site unable to connect to a business critical services or system. A business critical service that has failed affecting a single user and no alternative is available. Loss of main office script printers or printers used by dispensing practices when no alternative is available. GP PC when no alternative is available.</td>
<td>- Loss of COIN network connection for the whole site</td>
</tr>
<tr>
<td></td>
<td>- Non std equipment requests</td>
<td>- New software</td>
<td>- Software error</td>
<td>- Loss of main office script printers or printers used by dispensing practices when no alternative is available. GP PC when no alternative is available.</td>
<td>- Loss of telephone system for the whole site</td>
</tr>
<tr>
<td></td>
<td>- Installation of non std software/hardware</td>
<td>- New user accounts</td>
<td>- PC fault/failure</td>
<td>- Loss of Northern Ireland mail.</td>
<td>- Loss of email system for the whole site (excluding NHS mail.)</td>
</tr>
<tr>
<td></td>
<td>- Collection of redundant equipment</td>
<td>- Mobile phones Etc.</td>
<td>- Admin print/ fault failure</td>
<td>- Scanner fault/failure</td>
<td>- Std software fault/reinstall MS office, windows, adobe etc.</td>
</tr>
</tbody>
</table>
Table 3  Incident Rating

<table>
<thead>
<tr>
<th>Consequence score</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Negligible</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

Step 2 - Timeline for Managing Incidents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Negligible – incident to be noted and closed off within 5 days</td>
</tr>
<tr>
<td>2</td>
<td>Low – Incident manager to manage and close off incident within 5 days</td>
</tr>
<tr>
<td>3</td>
<td>Moderate - Incident manager to manage and close off incident within 5 days.</td>
</tr>
<tr>
<td>4</td>
<td>Major – Management response required from manager within 24 hours. (Note: If it is an IG incident refer to IG specialist immediately) Close off incident within 1 month. (If the close off target is not met an interim report of progress to be submitted to Corporate Governance &amp; Risk Officer</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic - Refer immediately to your Director and Specialist Officer. A management response is required as soon as possible within a 24hours period. Close off incident within 1 month. (If the close off target is not met an interim report of progress to be submitted to Corporate Governance &amp; Risk Officer</td>
</tr>
</tbody>
</table>

Specialist Contacts

<table>
<thead>
<tr>
<th>Specialist Contacts</th>
<th>Area</th>
<th>Emails Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health &amp; Safety Manager</td>
<td>Health and Safety/Fire/Env/Security</td>
<td><a href="mailto:necsu.healthandsafety@nhs.net">necsu.healthandsafety@nhs.net</a></td>
</tr>
<tr>
<td>Senior IG Officer</td>
<td>Information Governance</td>
<td><a href="mailto:necsu.ig@nhs.net">necsu.ig@nhs.net</a></td>
</tr>
<tr>
<td>Senior Governance Officer</td>
<td>Corporate Incidents</td>
<td><a href="mailto:necsu.sirmsoncidents@nhs.net">necsu.sirmsoncidents@nhs.net</a></td>
</tr>
<tr>
<td>Clinical Quality Team</td>
<td>Clinical Incidents</td>
<td><a href="mailto:necsu.qualitysafeguarding@nhs.net">necsu.qualitysafeguarding@nhs.net</a></td>
</tr>
</tbody>
</table>
Managers Incident Checklist

CCG Incident Investigating Manager’s Checklist

The Incident Investigating Manager has responsibility to act as Lead Investigator in any incident that involves their staff. Specialist advice and support on Information Governance and Health and Safety issues will be provided by NECS Governance Services, advice on provider quality issues will be provided by NECS Clinical Quality team.

It is important that lessons are learned from incidents which will help drive up standards across the organisation.

1. Do you know exactly what happened?
   - Talk to the person/people affected
   - Ensure you know exactly where and when the incident happened – this will be relevant to the investigation
   - If the incident involved equipment or furniture ensure these are retained but not used.
   - Offer support and reassurance

2. Has the incident led to a member of staff being absent from work?
   - If a staff member is absent from work for more than 7 days as a result of an incident that happened at work, the organisation must report this to the HSE through RIDDOR.
   - Inform NECS Senior Governance Officer (Health & Safety, Fire) who will make the RIDDOR report.

3. Have you identified the root cause of the incident?
   - Incidents may be caused by training need
   - It might be part of a wider issue
   - Ensure you have gathered sufficient evidence and documentation

4. Is a complaint likely to result from the incident?
   - Anticipating that a complaint might be made, apologising and explaining what steps you are going to take to correct a situation will often reduce the likelihood of a complaint being made.

5. Is the incident likely to lead to litigation?
   - All the information about the incident will be required in the event of a claim being made after an incident, it is therefore vital to ensure that every step taken has been fully documented and all documentation has been uploaded to SIRMS.

6. Have you put any immediate remedial measures in place?
   - Take steps to avoid a repeat of the incident
   - Ensure you have evidenced and documented the remedial measures
8. Rate the incident by its actual impact.
   □ Assess the impact of the incident on staff or the organisation
   □ If the incident was soft intelligence, select that option from the drop down list

9. Provide feedback to the person/people involved in the incident.
   □ Keep people informed of progress
   □ Offer reassurance
   □ Ensure you have evidence and documentation

10. Are you satisfied that all actions are complete?
     □ Upload all relevant documents to SIRMS
     □ Save and close
Appendix 10

Route Cause Analysis Guide

Root Cause Analysis Using Five Whys

What is it and how can it help me?

By repeatedly asking the question ‘why?’ (use five as a rule of thumb), you can peel away the layers of an issue, just like the layers of an onion, which can lead you to the root cause of a problem. The reason for a problem can often lead into another question; you may need to ask the question fewer or more than five times before you get to the origin of a problem. The real key is to avoid assumptions and logic traps and encourage the team to keep drilling down to the real root cause.

When does it work best?

By quickly identifying the source of an issue or problem, you can focus resources in the correct areas and ensure that you are tackling the true cause of the issue, not just its symptoms.

How to use it

How to complete the five whys
1. Write down the specific problem. Writing it down helps you formalise the problem and describe it accurately. It also helps a team focus on the same problem
2. Use brainstorming to ask why the problem occurs then, write the answer down below
3. If this answer doesn't identify the source of the problem, ask 'why?' again and write that answer down
4. Loop back to step three until the team agrees that they have identified the problem's root cause. Again, this may take fewer or more than five 'whys?'

Why use the five whys?
- Helps you to identify the root causes of a problem
- Helps you to determine the relationship between different root causes of a problem
- It is one of the simplest analysis tools as it's easy to complete without statistical analysis
- It is easy to learn and apply

Five whys and cause and effect diagrams

The five whys can either be used independently or as a part of a cause and effect diagram (fishbone diagram). The diagram helps you explore all potential or real causes which result in a failure or problem. Once you have established all the inputs on the cause and effect diagram, you can use the five whys technique to drill down to the root causes.

Tips
- Moving into ‘fix-it’ mode too quickly might mean dealing with symptoms but leaving the problem unresolved, so use the five whys to ensure that the cause of the problem is being addressed
- If you don’t ask the right questions, you don’t get the right answers. A question asked in the right way often points to its own answer
Example 1

A few years ago the Washington Monument (USA) was found to be disintegrating through erosion.

Why? Use of harsh chemicals Why? To clean pigeon poop Why? There were a lot of pigeons because pigeons eat spiders and there are a lot of spiders at monument Why? Spiders eat gnats and there were lots of gnats at monument Why? The gnats were attracted to the light at dusk and the monument was illuminated in the evening.

The root cause - The real issue wasn’t cleaning solutions, pigeons or spiders—it was gnats—which only come out at dusk. Dissuading them from doing so made all the other symptoms go away. Without identifying this, time and money would have been wasted by researching for solutions to the erosion which didn’t address the root cause which could have meant the monument would decay at a slower rate, but the damage would continue over time.

Solution/Lessons learned: Turn on the lights at a later time.

Example 2

Why? Complaint about dissatisfaction with a service to a customer. Why? Reports they had needed were not delivered in a timely manner. Why? SLA stated a particular date to deliver the reports. Why? The customer wanted reports outside this schedule. Why? There was no standard process for making changes to schedules and the contact was absent from work so the customer didn’t know who to contact.

The root cause – There was no clear process for making routine change requests and no alternative contact details had been passed on.

Solution/ Lessons learned – A standard form for submitting change requests has been created and the new process has been shared with both organisations and all relevant staff. A generic email address has been created (and this is now standard across all the team’s processes) and this will be constantly monitored by several staff.

Background
The five whys originated within Toyota as they developed their manufacturing methodologies. It forms a critical component of their problem solving training and is part of the induction into the Toyota production system. It is now also used within Six Sigma. Very often, the answer to the first ‘why?’ will prompt another ‘why?’ The answer to the second ‘why?’ will then prompt another and so on; hence the name, the five whys strategy.

Acknowledgements / sources
Six Sigma - Determining the Root Cause: 5 Whys , The Improvement Network
© Copyright NHS Institute for Innovation and Improvement 2008 © Copyright NHS Institute for Innovation and Improvement 2006-2013
Appendix 11

CCG Policy and Procedure Guidance for Reporting and Management of Serious Incidents (SIs) – via CCG