

## 

**Non-clinical incident &**

**Near- Miss Reporting Policy and Procedure**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Comment | Author |
| April 2020 | 1 | New Policy | Information Governance Team |
| June 2020 | 1 | Approved by NCL CCG Audit Committee | Information Governance Team |

**Document revision history**

Table of Contents

[Introduction 4](#_Toc43847575)

[Scope 5](#_Toc43847591)

[Purpose 5](#_Toc43847595)

[Equality Analysis 5](#_Toc43847596)

[Definitions 6](#_Toc43847597)

[Roles and Responsibilities 6](#_Toc43847598)

[Legal and Regulatory Reporting Requirements 7](#_Toc43847599)

[Process for Reporting and Managing Incidents 8](#_Toc43847600)

[Grading and Investigating Incidents 8](#_Toc43847601)

[Monitoring and Review 9](#_Toc43847602)

[Appendix 1: Incident Reporting Process and Flowchart 10](#_Toc43847603)

[Timescales 11](#_Toc43847604)

[Appendix 2: Low-Medium graded Incident Investigation form 12](#_Toc43847605)

[Annex One; Grading Matrix 15](#_Toc43847609)

[Appendix 3: High-Significant graded Incident 16](#_Toc43847610)

[Investigation form 16](#_Toc43847611)

[PART 1 (to be completed by incident reporter) **16**](#_Toc43847612)

[PART 2 (to be completed by Supervisor/ Manager) **18**](#_Toc43847613)

[Appendix 4: Risk Matrix Score 21](#_Toc43847614)

[Appendix 5: IG SIRI Breach Types Defined 27](#_Toc43847615)

[Information Governance Serious Incidents Requiring Investigation (IG SIRI); Breach Types 27](#_Toc43847616)

[Appendix 6: Clinical Serious Incident defined 32](#_Toc43847617)

# Introduction

## This document sets out the arrangements for reporting, managing, analysing and learning from incidents, accidents and near misses which arise from the activities of North Central London Clinical Commissioning Unit (NCL CCG), and sets out what NCL CCG expects from staff members who may be involved in reporting and managing incidents.

## Incidents can result in harm to staff and the public, damage to assets, disruption of activities and negative media attention. All incidents, including but not limited to…

## Accidents

## Near misses

## Property damage

## Equipment failure

## Information governance incidents including data loss and confidentiality breaches

## Violence, abuse or bullying

## …must be reported as soon as possible, as set out in the policy and reporting procedure.

## 

## Fair Blame statement;

## The response to incidents will focus on ‘what went wrong, not who went wrong’. Where errors have occurred and are openly reported, an investigation into the facts may take place but the disciplinary process will not be instigated in respect of any member of staff, except in the following circumstances:

## An incident where a fundamental breach of professional practice has occurred, and/or an incident which might lead any professional registration body to review the individual’s professional status

## Further occurrences of actions involving an individual who has previously received counselling, or been subject to disciplinary action related to the type of error that might have led to the incident

## Where it appears that staff may have been guilty of a criminal offence or some act or omission which may result in formal action by a regulatory or professional body

## Failure or significant delay in reporting an incident in which a member of staff was directly involved or were aware of

# 

# Scope

## This policy and procedure applies to; all staff employed by NCL CCG; to all third parties and others authorised to undertake work on behalf of NCL CCG.

## 

## For the purpose of this document a workplace is not just the NCL CCG own buildings, but anywhere a member of staff works from (including at home). If an incident occurs in a CCG, or other premises then their local procedure must be followed, in addition to the CCGs arrangements.

## 

## Staff concerns regarding the delivery of care or services, or the conduct of business, will be managed under the relevant Whistle Blowing Policy.

# 

# Purpose

All CCG staff have a duty to report incidents or near misses. The purpose of this policy is to;

* Provide NCL CCG staff with a single reference point to explain how incidents, accidents and near misses should be reported, in accordance organisational, legal and regulatory requirements.

The policy aims to:

* Enable prompt action to prevent recurrence of an incident or near miss
* Ensure that lessons are learned and communicated to aid the development of future safety strategies, safe systems of work and allocation of future resources
* Help identify health, safety and environmental risks and poor practices that may be prevented through the reporting procedure
* Provide an early warning for potential complaints or claims
* Inform the Risk Management Strategy and Risk Register
* Improve safety and security of staff and visitors

# 

# Equality Analysis

This document demonstrates the organisation’s commitment to create a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to use the Human Rights Act 1998 and to promote positive practice and value the diversity of all individuals and communities.

# 

# Definitions

For the purposes of this policy the following definitions apply:

Incident/Accident; any non-clinical event or omission that causes loss in any way for the organisation; physical or psychological injury to staff, visitors, members of the public. An incident could relate to one or more of the following:

* Security issue (incl. vandalism, property loss or damage)
* Fire or fire alarm activations
* Equipment
* Falls
* COSHH (Care of Substances Hazardous to Health)
* Vehicles
* Breach of confidentiality or inappropriate disclosure
* Failure to maintain professional registration

Near Miss; an incident that had the potential to cause harm but which was prevented.

Serious Incident; an incident that is graded as ‘High’ or ‘Significant’, using the risk categories contained within the form in Appendix Two.

# 

# Roles and Responsibilities

Corporate Governance team will:

* Provide advice and support to all employees involved in reporting and investigating incidents as appropriate;
* Provide reports to the Performance Delivery Internal Assurance Group (PDIAG) on a monthly basis as part of their assurance role;
* Ensure all staff are aware of the requirements for incident reporting via the provision of appropriate internal communications;
* Maintain records of reporting and investigating as appropriate.

Information Governance (IG) team will:

* Provide and support as appropriate on all IG related incidents;
* Ensure that external agencies are notified of any IG Serious Incident relating to Information Security as detailed within Appendix Five and facilitate the process thereafter.

Clinical Governance Team will:

* Ensure that external agencies are notified of any Serious Incident (excluding those relating to Information Security) as detailed within Appendix Four and facilitate the process thereafter.

All Partners and Senior Managers will:

* Ensure that staff are informed of the availability of the policy and cascade the information as required within their directorates.

All Staff

* Have a duty to report incidents or near misses in which they are involved or witness via the on-line reporting form

# 

# Legal and Regulatory Reporting Requirements

This policy is required to ensure compliance with the law and relevant regulatory and guidance requirements including, but not limited to:

* Management of Health and Safety at Work Regulations 1999.
* Reporting of Injuries, Diseases and Dangerous occurrences Regulations 1995, (RIDDOR).
* NHSE Serious Incident Framework
* NHS Counter Fraud Authority\*
* Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (Gateway Ref: 13177)

\*For further information on reporting incidents of fraud please refer to the NCL CCG Anti-Fraud, Bribery and Corruption policy.

# 

# Process for Reporting and Managing Incidents

Appendix One provides an Incident Reporting and Management flowchart which sets out the process and information flow of the arrangements for reporting, managing and investigating incidents and near misses which occur within NCL CCG.

When an incident or near miss occurs, the person reporting it must complete the information required on the on-line (via SUSI) form within 1 working day.

In the event of a fatality, major accident, case of disease or dangerous occurrence, or any other health & safety incident arising having potentially major implications, the Partner on call and the Corporate Governance Team should be notified as soon as possible.

# 

# Grading and Investigating Incidents

# Incidents are graded at a local level, and determined by the line manager / or area of responsibility within which the incident occurred. This triage process will determine the appropriate investigation response required.

The line manager responsible for the team / or area of responsibility within which the incident occurred will receive notification of the form within 48 hours, and be required to grade the incident, pending an investigation, proportionate to the level of the situation as below:

|  |  |
| --- | --- |
| Grade | Response |
| Low – Medium Risk | Incident investigated locally by line manager\* |
| High – Significant Risk | Incident must be immediately notified to the Corporate Governance team, in addition to the lead Partner / Partner on-call\* |

\*If the matter relates to an information incident or a patient safety incident it must be reported immediately to the relevant manager of the service and to NCL CCG Information Governance Hub (NELCSU.informationgoverance@nhs.net) or Clinical Governance team (slcsu.si@nhs.net)

If there is a possibility that a risk remains, it is essential that a risk assessment is undertaken, with the risk added to the relevant risk register.

If there is any doubt as to what remedial action should be taken, the Line Manager should seek advice from the relevant person e.g. Health & Safety Advisor, Fire Safety Officer, LSMS or Information Governance Manager.

As a general principle, the depth and vigour of an investigation should be proportionate to the level of risk and grading of the incident. To ensure the proportionality of investigation and reporting, Appendix Two sets out the proforma for the level of reporting required for low - medium graded incidents. Appendix Three sets out the proforma for the level of reporting required for high – significant graded incidents.

# 

# Monitoring and Review

Reports will be presented for review on a monthly basis to the NCL CCG Performance Delivery Internal Assurance Group (PDIAG or Assurance group), to seek assurance that appropriate measures are taken to prevent incidents from recurring. ‘Lessons learned’ will be used to inform the development of future procedural documents.

This policy will be reviewed on a yearly basis.

# Appendix 1: Incident Reporting Process and Flowchart

**INCIDENT/ACCIDENT/ NEAR MISS OCCURS**

Notify outside agencies as applicable (within timescales)

Identification of lead Investigator

Line manager / responsible area accesses on-line report within 48 hours. Incident reviewed and graded (risk assessed) \*\*

Incident reported via on-line form completed by member of staff involved in or witness to event, within 1 working day.

Immediate verbal report to line manager/responsible service lead\*

***Member of staff preserves any evidence, equipment or documentation***

***Consider immediate needs of staff***

***Automatic onward notification to Corporate Governance Team who notify the line manager***

***Accessed via SUSI***

**Incident graded High-Significant**

**Incident graded Low-Medium**

Line Manager Investigation (as per Appendix 2)

Immediate verbal report to appropriate Partner and Corporate Governance Team (or on-call Partner).

Onward notification and referral as appropriate to type of incident or near miss

Investigation & follow up

***Incident declared on StEIS and report through the SI process***

* Action plan & report completed as required and attached to incident
* Incident closed on reporting system
* Learning cascaded as applicable

***Update StEIS with further information***

\*If the matter relates to an information incident or a patient safety incident it must be reported immediately to the relevant manager of the service and to NCL CCGS’s IG (NCL CCGS.informationgoverance@nhs.net) or Clinical Governance team (slcsu.si@nhs.net)

\*\* For incidents graded as serious, the relevant Accountable Partner will appoint the investigating officer.

## Timescales

Investigation commences as soon after the incident occurs as possible. Reporting and investigation to commence immediately if incident relates to information loss or security breach or affects patient safety. If the investigation is likely to take more than 2 weeks, the appropriate Partner / Corporate Governance team will be advised). Investigation report completed within 10 days of the conclusion of the investigation and considered by the relevant Partner.

# Appendix 2: Low-Medium graded Incident Investigation form

## The grading and level of investigation progressed in line with an incident will be reviewed and approved/rejected by the NCL CCG Performance Delivery Internal Assurance Group (PDIAG).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Incident description and consequences  (include how the incident was detected) |  | | | | | | | |
| Effect on patient | Yes  (provide detail, including involvement and support of patient and relatives) | | Not applicable | | | | | |
| Effect on service delivery | Low  Moderate  High  Very High | | Anything above ‘Low’ please provide further details | | | | | |
| Date of Incident |  | | | | | | | |
| Incident Reporter  (name and title) |  | | Contact email and telephone: | | | | | |
| Investigating Manager  (name and title) |  | | Contact email and telephone: | | | | | |
| Contact email and telephone: |  | | | | | | | |
| Risk Score\* (Impact x Likelihood)  please complete | Impact |  | Likeli-hood |  | Score | | |  |
| Incident (Risk) Grading\*  (tick as appropriate) | Low  (1-3) |  | Medium  (4-6) |  | High  (8-12)# |  | Very High  (15-25)\* |  |
| Cause of Incident  (What factors do you think caused the incident to happen?) |  | | | | | | | |
|  | Chronology (timeline) of events;   |  |  | | --- | --- | | Date/Time | Event | |  |  | | | | | | | | |
|  | Contributing factors | | | | | | | |
| Outcome of investigation (Action to reduce likelihood of a similar recurrence. Please address each causal factor above) | Analysis of root cause | | | | | | | |
| Lessons Learned (action to share learning). | | | | | | | |
| Recommendations (e.g. amend Standard Operating Procedures / remind team members / induction of new staff). | | | | | | | |
| Agreed actions | |  |  |  | | --- | --- | --- | | Action | By When | Lead | |  |  |  | |  |  |  | | | | | | | | |

## 

## \*Refer to Annex One below for the grading matrix.

## 

## If the incident is graded High / Very High, a full investigation form as contained within the policy must be completed. Further information can be obtained via the NELCSU portal or by calling Jay Patel, Principal Associate, Corporate Affairs on ext 379361 or emailing [NELCSU.reporting@nhs.net](mailto:NELCSU.reporting@nhs.net)

## Annex One; Grading Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| POTENTIAL SEVERITY - Please grade the impact were this incident to happen again, along with the likelihood of it happening given the actions you have now taken using the table below. | | | | | | |
| Assessment of Overall Risk Score and RAG Grading | | | | | | |
| Impact | Very High | **R**  (5) | **R**  **(10)** | **R**  **(15)** | **R**  **(20)** | **R**  **(25)** |
| High | **A**  **(4)** | **A**  **(8)** | **A/R**  **(12)** | **R**  **(16)** | **R**  **(20)** |
| Medium | **A/G**  **(3)** | **A**  (6) | **A**  **(9)** | **A/R**  **(12)** | **A/R**  **(15)** |
| Low | **G**  **(2)** | **A/G**  **(4)** | **A/G**  **(6)** | **A**  **(8)** | **A**  **(10)** |
| Very Low | **G**  **(1)** | **G**  **(2)** | **G**  **(3)** | **G**  **(4)** | **G**  **(5)** |
| R – Red  A – Amber  G - Green | | **Rare**  **1** | **Unlikely**  **2** | **Possible**  **3** | **Likely**  **4** | **Almost Certain**  **5** |
| **Likelihood** | | | | |

# Appendix 3: High-Significant graded Incident

## 

## Investigation form

Details in this form should only be facts only – no opinions should be given.

Those completing this form should do so using Black Ink, print their name, sign and keep within the boxes provided.

### 

### **PART 1 (to be completed by incident reporter)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Affected Personal Details** | | | |
| First Name |  | Sur-name |  |
| Contact Details  Telephone, Mobile, Email |  | Job Title  (if staff) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Details** | | | | |
| Date |  | | Time |  |
| Location |  | | | |
| Description of event (give a brief description of the incident. Only state facts about the incident. If equipment were involved, please give as much information as possible. Please also include a police crime reference number, (if applicable). | | | | |
| Details of any witnesses | | | | |
| Name | | Title (job title if member of staff) | | Contact details |
|  | |  | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK GRADE IMPACT OF INCIDENT (please circle the most appropriate grade – refer to the Risk Impact Assessment (examples at the end of form).** | | | |
| Low Risk  (1-3) | Medium Risk  (4-6) | High Risk  (8-12) | Significant Risk  (15-25) |

If the risk rating of an incident is of a Very High Impact e.g. involving a death, staff member should contact Line Manager / Supervisor IMMEDIATELY to ensure matter has been reported as a Serious Incident.

|  |  |  |  |
| --- | --- | --- | --- |
| **INCIDENT REPORTER DETAILS** | | | |
| Name | Signature | Date | Contact Telephone number and e-mail |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Please give this form to your manager (or person acting as manager in their absence) as soon as you have completed Part 1. They will then need to complete Part 2.** | | |
| Name of Manager | Job Title | Date Sent |
|  |  |  |

### **PART 2 (to be completed by Supervisor/ Manager)**

|  |  |
| --- | --- |
| **More about the incident** | |
| Incident or Near Miss | Incident  Near Miss  (Tick one) |
| Type of Incident / Near Miss | Tick one of the following which best describes the incident / near miss  Tenants, patients, visitor or public  NCL CCG staff  NCL CCG Contractors  Equipment or premises or IT systems failure  Information Security Breach |
| Type of Location | Tick one of the following which best describes the incident / near miss  Health Centre  Dental Practice  GP Surgery  Community Trust / Hospital  Office / Administration Building  Leisure Facility  Grounds / Car Park  Other |
| Immediate Response to Incident | (Enter action taken at the time of the incident) |
| Did the incident result in staff absence?  If YES – Please state anticipated absence from work or incapacity (RIDDOR) |  |
| Name of Line Manager Informed |  |
| Risk Grade Incident |  |

**Local Management Review / Investigation of Incident**

|  |
| --- |
| **OUTCOME OF INCIDENT (Please describe what happened as a result of the incident)** |
|  |

|  |
| --- |
| **CONTRIBUTORY FACTORS (What do you think caused the incident to happen?)** |
|  |

|  |
| --- |
| **ACTIONS TAKEN TO REDUCE THE LIKELIHOOD OF A SIMILAR INCIDENT RECURRING (Please make sure you address all the contributory factors identified)** |
|  |

|  |
| --- |
| **Further Action** |
| Have police been informed (if applicable)  Give police Crime reference No:  Have staff involved been given feedback?  Is the learning applicable elsewhere?  If no further action - Can this incident be CLOSED? |

Please send a completed copy of pages 1 and 2 to the Governance Team

# Appendix 4: Risk Matrix Score

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Table header | | | | |
| Table text | 1 | 2 | 3 | 4 | 5 |
| Domains | Negligible | Minor | Moderate | Major | Catastrophic` |
| Impact on the safety of patients, staff or public (physical/ psychological harm) | Minimal injury requiring no/minimal intervention or treatment.  No time off work | Minor injury or illness, requiring minor intervention  Requiring time off work for >3 days  Increase in length of hospital stay by 1-3 days | Moderate injury requiring professional intervention  Requiring time off work for 4-14 days  Increase in length of hospital stay by 4-15 days  RIDDOR/ agency reportable incident  An event which impacts on a small number of patients | Major injury leading to long-term incapacity/disability  Requiring time off work for >14 days  Increase in length of hospital stay by >15 days  Mismanagement of patient care with long-term effects | Incident leading to death  Multiple permanent injuries or irreversible health effects  An event which impacts on a large number of patients |
| Quality/ complaints/ audit | Peripheral element of treatment or service suboptimal  Informal complaint/  inquiry | Overall treatment or service suboptimal  Formal complaint (stage 1)  Local resolution  Single failure to meet internal standards  Minor implications for patient safety if unresolved  Reduced performance rating if unresolved | Treatment or service has significantly reduced effectiveness  Formal complaint (stage 2) complaint  Local resolution (with potential to go to independent review)  Repeated failure to meet internal standards  Major patient safety implications if findings are not acted on | Non-compliance with national standards with significant risk to patients if unresolved  Multiple complaints/ independent review  Low performance rating  Critical report | Totally unacceptable level or quality of treatment/service  Gross failure of patient safety if findings not acted on  Inquest/ombudsman inquiry  Gross failure to meet national standards |
| Human resources/ organisational development/ staffing/ competence | Short-term low staffing level that temporarily reduces service quality (< 1 day) | Low staffing level that reduces the service quality | Late delivery of key objective/ service due to lack of staff  Unsafe staffing level or competence (>1 day)  Low staff morale  Poor staff attendance for mandatory/key training | Uncertain delivery of key objective/service due to lack of staff  Unsafe staffing level or competence (>5 days)  Loss of key staff  Very low staff morale  No staff attending mandatory/ key training | Non-delivery of key objective/ service due to lack of staff  On-going unsafe staffing levels or competence  Loss of several key staff  No staff attending mandatory training /key training on an on-going basis |
| Statutory duty/ inspections | No or minimal impact or breach of guidance/ statutory duty | Breach of statutory legislation  Reduced performance rating if unresolved | Single breach in statutory duty  Challenging external recommendations/ improvement notice | Enforcement action  Multiple breaches in statutory duty    Improvement notices  Low performance rating  Critical report | Multiple breaches in statutory duty  Prosecution  Complete systems change required  Zero performance rating  Severely critical report |
| Adverse publicity/ reputation | Rumours  Potential for public concern | Local media coverage – short-term reduction in public confidence  Elements of public expectation not being met | Local media coverage – long-term reduction in public confidence | National media coverage with <3 days service well below reasonable public expectation | National media coverage with >3 days service well below reasonable public expectation.  MP concerned (questions in the House)  Total loss of public confidence |
| Business Projects/ Objectives | Insignificant cost increase/ schedule slippage  Key ‘political’ target is being achieved and impact prevents improvement | <5 per cent over project budget  Schedule slippage  Key ‘political’ target is being achieved but impact reduces performance marginally below target in the near future or  Performance currently on target, but there is no agreed plan to meet the target | 5–10 per cent over project budget  Schedule slippage  Key ‘political’ goal is marginally below target or is soon projected to deteriorate beyond acceptable limits or  There is an agreed plan, but it does not yet meet the rising target | Non-compliance with national 10–25 per cent over project budget  Schedule slippage  Key ‘political’ target not being achieved, and impact prevents improvement, or substantial decline in performance trend | Incident leading >25 per cent over project budget  Schedule slippage  Key objectives not met  Key ‘political’ target is not being achieved and the impact further deteriorates the position |
| Finance including claims | Small loss Risk of claim remote | Loss of 0.1–0.25 per cent of budget  Claim less than £10,000 | Loss of 0.25–0.5 per cent of budget  Claim(s) between £10,000 and £100,000 | Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget  Claim(s) between £100,000 and £1 million  Purchasers failing to pay on time | Non-delivery of key objective/ Loss of >1 per cent of budget  Failure to meet specification/ slippage  Loss of contract / payment by results  Claim(s) >£1 million |
| Service/business interruption Environmental impact | Loss/interruption of >1 hour  Minimal or no impact on the environment | Loss/interruption of >8 hours    Minor impact on environment | Loss/interruption of >1 day  Moderate impact on environment | Loss/interruption of >1 week  Major impact on environment | Permanent loss of service or facility  Catastrophic impact on environment |

Table 2 Likelihood score (L)

What is the likelihood of the consequence occurring?

The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency.

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

For grading risk, the scores obtained from the risk matrix are assigned grades as follows

Table 3 Risk scoring = consequence x likelihood ( C x L )

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood | | | | |
| Likelihood score | 1 | 2 | 3 | 4 | 5 |
|  | Rare | Unlikely | Possible | Likely | Almost certain |
| 5 Catastrophic | 5 | 10 | 15 | 20 | 25 |
| 4 Major | 4 | 8 | 12 | 16 | 20 |
| 3 Moderate | 3 | 6 | 9 | 12 | 15 |
| 2 Minor | 2 | 4 | 6 | 8 | 10 |
| 1 Negligible | 1 | 2 | 3 | 4 | 5 |

For grading risk, the scores obtained from the risk matrix are assigned grades as follows

|  |  |  |
| --- | --- | --- |
|  | | |
|  | 1 - 3 | Low risk |
|  | 4 - 6 | Medium risk |
|  | 8 - 12 | High risk |
|  | 15 - 25 | Very High risk |

# Appendix 5: IG SIRI Breach Types Defined

## 

## Information Governance Serious Incidents Requiring Investigation (IG SIRI); Breach Types

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’.

These more detailed definitions and examples should help IG Incident Reporting. Users select the most appropriate ‘Breach Type’ category when completing the IG SIRI record on the online tool. However, it is recognised that many data incidents will involve elements of one or more of the following categories. For the purpose of reporting, the description which best fits the key characteristic of the incident should be selected.

Although the primary factors for assessing the severity level are the numbers of individual data subjects affected, the potential for media interest, and the potential for reputational damage, other factors may indicate that a higher rating is warranted, for example the potential for litigation or significant distress or damage to the data subject(s) and other personal data breaches of the Data Protection Act. As more information becomes available, the IG SIRI level should be re-assessed.

Source; Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation V5.1 – 29th May 2015

|  |  |
| --- | --- |
| **Breach Type** | **Examples / incidents covered within this definition** |
| Lost in Transit | The loss of data (usually in paper format, but may also include CD’s, tapes, DVD’s or portable media) whilst in transit from one business area to another location. May include data that is;   * Lost by a courier; * Lost in the ‘general’ post (i.e. does not arrive at its intended destination); * Lost whilst on site but in situ between two separate premises / buildings or departments; * Lost whilst being hand delivered, whether that be by a member of the data controller’s staff or a third party acting on their behalf   Generally speaking, ‘lost in transit’ would not include data taken home by a member of staff for the purpose of home working or similar (please see ‘lost or stolen hardware’ and ‘lost or stolen paperwork’ for more information). |
| Lost or stolen hardware | The loss of data contained on fixed or portable hardware. May  include;   * Lost or stolen laptops; * Hard-drives; * Pen-drives; * Servers; * Cameras; * Mobile phones containing personal data; * Desk-tops / other fixed electronic equipment; * Imaging equipment containing personal data; * Tablets; * Any other portable or fixed devices containing personal data;   The loss or theft could take place on or off a data controller’s  premises. For example, the theft of a laptop from an employee’s home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk. |
| Lost or stolen paperwork | The loss of data held in paper format. Would include any paper work lost or stolen which could be classified as personal data (i.e. is part of a relevant filing system/accessible record). Examples would include;   * medical files; * letters; * rotas; * ward handover sheets; * employee records   The loss or theft could take place on or off a data controller’s premises, so for example the theft of paperwork from an employee’s home or car or a loss whilst they were travelling on public transport would be included in this category.  Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system). |
| Disclosed in Error | This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information itself hasn’t actually been accessed. Examples include:   * Letters / correspondence / files sent to the incorrect individual; * Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s55 aspect of reporting below); * Failure to redact personal data from documentation supplied to third parties; * Inclusion of information relating to other data subjects in error; * Emails or faxes sent to the incorrect individual or with the incorrect information attached; * Failure to blind carbon copy (‘bcc’) emails; * Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data; * Disclosure of data to a third party contractor / data processor who is not entitled to receive it |
| Uploaded to website in error | This category is distinct from ‘disclosure in error’ as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include;   * Failures to carry out appropriate redactions; * Uploading the incorrect documentation; * The failure to remove hidden cells or pivot tables when uploading a spreadsheet; * Failure to consider / apply FOIA exemptions to personal data |
| Non-secure Disposal – hardware | The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include;   * Failure to meet the contracting requirements of principle seven when employing a third party processor to carry out the removal / destruction of data; * Failure to securely wipe data ahead of destruction; * Failure to securely destroy hardware to appropriate industry standards; * Re-sale of equipment with personal data still intact / retrievable; * The provision of hardware for recycling with the data still intact |
| Non-secure Disposal – paperwork | The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include;   * Failure to meet the contracting requirements of principle seven when employing a third party processor to remove / destroy / recycle paper; * Failure to use confidential waste destruction facilities (including on site shredding); * Data sent to landfill / recycling intact – (this would include refuse mix up’s in which personal data is placed in the general waste); |
| Technical security failing (including hacking) | This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include:   * Failure to appropriately secure systems from inappropriate / malicious access; * Failure to build website / access portals to appropriate technical standards; * The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of industry best practice; * Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces); * Failure to implement appropriate controls for remote system access for employees (for example when working from home)   In respect of successful hacking attempts, the ICO’s interest is in whether there were adequate technical security controls in place to mitigate this risk.  **A technical security incident may also be a Cyber incident (please see Cyber guidance within this document)** |
| Corruption or inability to recover electronic data | Avoidable or foreseeable corruption of data or an issue which  otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care / adverse clinical outcomes.  For example;   * The corruption of a file which renders the data inaccessible; * The inability to recover a file as its method / format of storage is obsolete; * The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible |
| Unauthorised access/disclosure | The offence under section 55 of the DPA - willful unauthorised  access to, or disclosure of, personal data without the consent of the data controller.  Example (1)  An employee with admin access to a centralised database of  patient details, accesses the records of her daughter’s new boyfriend to ascertain whether he suffers from any serious medical conditions. The employee has no legitimate business need to view the documentation and is not authorised to do so. On learning that the data subject suffers from a GUM related medical condition, the employee than challenges him about his sexual history.  Example (2)  An employee with access to details of patients who have sought treatment following an accident, sells the details to a claims company who then use this information to facilitate lead generation within the personal injury claims market. The employee has no legitimate business need to view the documentation and has committed an offence in both accessing the information and in selling it on.  A recent successful prosecution for a s55 offence:  http://ico.org.uk/news/latest\_news/2013/gp-surgery-manager- prosecuted-for-illegally-accessing-patients-medical-records-  02122013 |
| Other | This category is designed to capture the small number of occasions on which a principle seven breach occurs which does not fall into the aforementioned categories. These may include:   * Failure to decommission a former premises of the data controller by removing the personal data present; * The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data; * Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets).   This category also covers all aspects of the remaining data protection principles as follows:   * Fair processing; * Adequacy, relevance and necessity; * Accuracy; * Retaining of records; * Overseas transfers |

# Appendix 6: Clinical Serious Incident defined

Source: Serious Incident Framework, NHSE (March 215)

In broad terms, serious incidents are events in health care where the potential for learning is so great, or the consequences to patients, families and carers, staff or organisations are so significant, that they warrant using additional resources to mount a comprehensive response. Serious incidents can extend beyond incidents which affect patients directly and include incidents which may indirectly impact patient safety or an organisation’s ability to deliver ongoing healthcare.

The occurrence of a serious incident demonstrates weaknesses in a system or process that need to be addressed to prevent future incidents leading to avoidable death or serious harm[[1]](#footnote-1) to patients or staff, future incidents of abuse to patients or staff, or future significant reputational damage to the organisations involved. Serious incidents therefore require investigation in order to identify the factors that contributed towards the incident occurring and the fundamental issues (or root causes) that underpinned these. Serious incidents can be isolated, single events or multiple linked or unlinked events signalling systemic failures within a commissioning or health system.

There is no definitive list of events/incidents that constitute a serious incident and lists should not be created locally as this can lead to inconsistent or inappropriate management of incidents. Where lists are created there is a tendency to not appropriately investigate things that are not on the list even when they should be investigated, and equally a tendency to undertake full investigations of incidents where that may not be warranted simply because they seem to fit a description of an incident on a list.

The definition below sets out circumstances in which a serious incident must be declared. Every incident must be considered on a case-by-case basis using the description below. Inevitably, there will be borderline cases that rely on the judgement of the people involved (see section 1.1).

Serious Incidents in the NHS include:

* Acts and/or omissions occurring as part of NHS-funded healthcare (including in the community) that result in:
* Unexpected or avoidable death[[2]](#footnote-2) of one or more people. This includes
* suicide/self-inflicted death; and
* homicide by a person in receipt of mental health care within the recent past[[3]](#footnote-3) (see Appendix 1);
* Unexpected or avoidable injury to one or more people that has resulted in serious harm;
* Unexpected or avoidable injury to one or more people that requires further treatment by a healthcare professional in order to prevent:—
* the death of the service user; or
* serious harm;
* Actual or alleged abuse; sexual abuse, physical or psychological ill-treatment, or acts of omission which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery where:
* healthcare did not take appropriate action/intervention to safeguard against such abuse occurring[[4]](#footnote-4) ; or
* where abuse occurred during the provision of NHS-funded care.

This includes abuse that resulted in (or was identified through) a Serious Case Review (SCR), Safeguarding Adult Review (SAR), Safeguarding Adult Enquiry or other externally-led investigation, where delivery of NHS funded care caused/contributed towards the incident (see Part One; sections 1.3 and 1.5 for further information).

* A Never Event - all Never Events are defined as serious incidents although not all Never Events necessarily result in serious harm or death. See Never Events Policy and Framework for the national definition and further information[[5]](#footnote-5);
* An incident (or series of incidents) that prevents, or threatens to prevent, an organisation’s ability to continue to deliver an acceptable quality of healthcare services, including (but not limited to) the following:
* Failures in the security, integrity, accuracy or availability of information often described as data loss and/or information governance related issues (see Appendix 2 for further information);
* Property damage;
* Security breach/concern[[6]](#footnote-6);
* Incidents in population-wide healthcare activities like screening[[7]](#footnote-7) and immunisation programmes where the potential for harm may extend to a large population;
* Inappropriate enforcement/care under the Mental Health Act (1983) and the Mental Capacity Act (2005) including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS);
* Systematic failure to provide an acceptable standard of safe care (this may include incidents, or series of incidents, which necessitate ward/ unit closure or suspension of services[[8]](#footnote-8)); or
* Activation of Major Incident Plan (by provider, commissioner or relevant agency)[[9]](#footnote-9)
* Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation[[10]](#footnote-10).

1. Serious harm:

   Severe harm (patient safety incident that appears to have resulted in permanent harm to one or more persons receiving NHS-funded care);

   Chronic pain (continuous, long-term pain of more than 12 weeks or after the time that healing would have been thought to have occurred in pain after trauma or surgery ); or

   Psychological harm, impairment to sensory, motor or intellectual function or impairment to normal working or personal life which is not likely to be temporary (i.e. has lasted, or is likely to last for a continuous period of at least 28 days). [↑](#footnote-ref-1)
2. Caused or contributed to by weaknesses in care/service delivery (including lapses/acts and/or omission) as opposed to a death which occurs as a direct result of the natural course of the patient’s illness or underlying condition where this was managed in accordance with best practice. [↑](#footnote-ref-2)
3. This includes those in receipt of care within the last 6 months but this is a guide and each case should be considered individually - it may be appropriate to declare a serious incident for a homicide by a person discharged from mental health care more than 6 months previously. [↑](#footnote-ref-3)
4. This may include failure to take a complete history, gather information from which to base care plan/treatment, assess mental capacity and/or seek consent to treatment, or fail to share information when to do so would be in the best interest of the client in an effort to prevent further abuse by a third party and/or to follow policy on safer recruitment. [↑](#footnote-ref-4)
5. Never Events arise from failure of strong systemic protective barriers which can be defined as successful, reliable and comprehensive safeguards or remedies e.g. a uniquely designed connector to prevent administration of a medicine via the incorrect route - for which the importance, rationale and good practice use should be known to, fully understood by, and robustly sustained throughout the system from suppliers, procurers, requisitioners, training units, and front line staff alike. See the Never Events Policy and Framework available online at: http://www.england.nhs.uk/ourwork/patientsafety/never-events/ [↑](#footnote-ref-5)
6. This will include absence without authorised leave for patients who present a significant risk to themselves or the public. [↑](#footnote-ref-6)
7. Updated guidance will be issued in 2015. Until that point the Interim Guidance for Managing Screening Incidents (2013) should be followed. [↑](#footnote-ref-7)
8. It is recognised that in some cases ward closure may be the safest/ most responsible action to take but in order to identify problems in service/care delivery , contributing factors and fundamental issues which need to be resolved an investigation must be undertaken [↑](#footnote-ref-8)
9. For further information relating to emergency preparedness, resilience and response, visit: <http://www.england.nhs.uk/ourwork/eprr/> [↑](#footnote-ref-9)
10. As an outcome loss in confidence/ prolonged media coverage is hard to predict. Often serious incidents of this nature will be identified and reported retrospectively and this does not automatically signify a failure to report. [↑](#footnote-ref-10)