APPROVED

NHS
Health Education England

Incident Reporting Policy

Version:	2.0
Ratified by:	HEE Exec Team
Date ratified:	26 March 2019
Name and Title of originator/author(s):	Mike Jones, Head of Corporate Assurance Andrew Todd, Information Governance Lead
Name of responsible Director:	Lee Whitehead, Director of People and Communications
Date issued:	
Review date:	26 March 2021
Target audience:	HEE Staff
Document History:	Reviewed by: IGSG May 2016, March 2017, May 2017, May 2018 SERCO ASP Safety Team August 2016 HEE Exec Team March 2019

Developing people
for health and
healthcare

www.hee.nhs.uk

(BLANK PAGE)

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Executive Summary

The objectives of this policy are to:

Ensure that HEE manages and investigates all incidents in accordance with best practice, learns and shares lessons from them and takes appropriate action to protect patients, staff, contractors, volunteers and members of the public from harm by: recording adverse incidents; investigating incidents as appropriate; regular monitoring of incident data and appropriate reporting to the Audit Committee; timely and effective reporting to statutory agencies; promoting a just and fair culture; minimising loss of reputation, or assets; ensuring that lessons are learned from incidents to prevent such incidents recurring; and ensuring that Health Education England (HEE) complies with current legislation, policies and best practice.

Ensure the Senior Information Risk Owner (SIRO) is aware of information security incidents and cyber security incidents.

Ensure a standardised approach to the management of Information Governance and Cyber Security incidents within HEE.

Ensure that learning from incidents is an integral part of HEE's culture and provide a process to ensure information to the accountable officer is available regarding incidents where fraudulent activity is suspected.

Promote a culture of accountability without 'blame'.

To improve staff and service user's data security by addressing systematic errors

Contents

1. Introduction

1.1 Health Education England (HEE) is committed to ensuring that an incident reporting system is in place as part of its approach to risk management, so that HEE can learn from incidents to improve safety within the organisation. Incidents may occur in any area of the organisation or within commissioned services and may be clinical or non-clinical in nature. Reporting incidents will enable HEE to meet legal compliance, identify trends and take positive action to prevent or minimise the likelihood of the error or incident recurring in the future.

1.2 This policy is one of a set that support the delivery of the organisation's approach to risk management and is underpinned by the following policies and procedures:

- The Information Governance & Cyber Security Incident Management and Reporting Procedures
- The Investigation Procedure
- The Serious Incident Requiring Investigation Procedure
- Health & Safety Policy
- Incident Reporting including RIDDOR (Health & Safety) SOP
- Information Risk Management Policy
- Business Continuity Policy
- Information Security Policy
- Data Protection Policy
- Records Management Policy

1.3 Taken together they achieve the following:

- Clarification of roles and responsibilities of staff regarding the management of incidents;
- Setting of standards regarding investigation and analysis; and
- Setting of standards regarding the development and implementation of risk reduction strategies.

2. Aims & Objectives

2.1 HEE aims to be an organisation with a memory to learn lessons from its incidents. The objective of this policy is to ensure that HEE manages and investigates all incidents in accordance with best practice, learns and shares lessons from them and takes appropriate action to protect patients, staff contractors, volunteers and members of the public from harm by:

- recording adverse incidents;
- investigating incidents as appropriate;
- regular monitoring of incident data and appropriate reporting to the Audit Committee;
- timely and effective reporting to statutory agencies;
- promotion of a just and fair culture;
- minimising loss of reputation, or assets;
- ensuring that lessons are learned from incidents to prevent such incidents recurring; and
- ensuring that HEE complies with current legislation, policies and best practice
- Ensuring the SIRO is aware of information security incidents and cyber security incidents
- Ensuring a standardised approach to the management of Information Governance (IG) and cyber security incidents within HEE
- Ensuring that learning from incidents is an integral part of HEEs culture
- Providing information to the accountable officer regarding incidents where fraudulent activity is suspected.
- Promoting a culture of accountability without 'blame'

2.2 The principles underlying HEE's approach are given below:

a) Ensuring Confidentiality

2.3 The incident reporting forms may include personal and sensitive information. All information relating to incidents will be stored securely in accordance with the General Data Protection Regulation (GDPR) and the UK's Data Protection Act, and will conform to HEE's Records Management Policy. Staff should use O365 as a secure way of sharing a completed incident form wherever possible. Should documents need to be posted, staff must use a sealed envelope and mark it confidential.

2.4 Any requests to keep an individual's identity confidential will be respected as far as possible and in line with current legislation

b) Learning from Incidents

2.5 An accident or incident, however serious, is rarely caused wilfully, although staff can inadvertently trigger a cyber-attack by accessing personal email accounts or fraudulent websites. Errors are often caused by a number of factors, including, but not limited to, process problems, human factors, individual behavior and lack of knowledge or skills. Learning from such incidents can only take place when they are reported and investigated in a positive, open and structured way. Determining safe practice is an important part of

successful risk management. Avoiding blame and adopting a culture of learning from incidents, will promote a fair and open culture and a safe environment throughout the organisation.

2.6 HEE aims to ensure, as far as reasonably practicable, there is appropriate learning from incidents. Incidents will be investigated as appropriate to ascertain the root cause of the problem and to enable HEE to learn from any mistakes, minimising the risk of recurrence.

2.7 HEE will investigate and manage all IG and cyber security incidents and provide staff with guidelines on identifying and reporting information incidents including near-misses.

2.8 This policy ensures Caldicott 2 recommendations are addressed and contractual obligations are adhered to with regards to managing, investigating and reporting within a standardised and consistent manner.

2.9 All IG and cyber security incidents will be investigated, assessed, categorised and reported using NHS Digital's *'Guide to the Notification of Data Security and Protection Incidents'*.

c) Just and Fair Culture

2.10 HEE is committed to promoting an open and fair culture where staff feel able to report incidents or near misses and learn from mistakes without fear of recrimination.

2.11 All staff will be encouraged to recognise potential risks and feel supported in the reporting of an event (whether an incident or a near miss) in a fair blame culture. Exceptions to this are where the organisation's policies and guidelines are deliberately breached or there is willful misconduct or negligence.

3. Scope

3.1 This policy and procedure must be followed by all staff who carry out work for HEE, including while on another organisation's premises or staff who are injured while travelling during their working hours. This includes staff on temporary or honorary contracts, secondments, pool staff and students. It also applies to volunteers, visitors and contractors.

3.2 There are two pathways by which incidents are reported and subsequently managed depending on the type of incident. The pathways are:

- Information Governance and Cyber Security incidents as detailed in Annex A to C of the Information Governance and Cyber Security Incident Management and Reporting Procedure document.
- Health & Safety Incidents as detailed in the Incident Reporting including RIDDOR (Health & Safety) SOP

4. Accountability

4.1 The Chief Executive is responsible for the policy.

4.2 The Audit Committee is responsible for monitoring compliance with the policy and will receive regular reports on incidents reported.

4.3 The Executive Team will monitor the incident reports.

4.4 The Audit Committee will be made aware of reports on incidents reported under the policy to enable trends and patterns to be identified. An annual risk management report will also summarise incidents reported under the policy in the year and identify any trends and lessons learned. The Audit Committee will also be informed on a quarterly basis regarding incidents via a Quarterly Report.

5. Chief Executive

5.1 The Chief Executive has overall accountability for risk management and the safety of patients, visitors and staff. The Chief Executive is ultimately responsible for ensuring all investigations are dealt with appropriately.

6. Directors

6.1 Each Director is responsible for:

- **a)** ensuring appropriate arrangements are in place for implementing the incident reporting procedure in their areas of responsibility;
- **b)** providing help and support to all staff who investigate incidents;
- **c)** ensuring that risks identified within their Directorate are acted upon
- **d)** creating an open and fair culture; and
- **e)** escalating adverse events according to the risk rating score.

7. Director of Finance

7.1 The Director of Finance is the accountable officer for incidents where fraudulent activity is suspected including cyber security, all such information should be reported to the Director of Finance with immediate effect. In the absence of the Director of Finance such matters may be reported to the Local Counter Fraud Specialist (LCFS) or the National Fraud Reporting line. Please refer to HEE's Counter-Fraud and Anti-Bribery Policy.

7.2

8. Senior Information Risk Owner (SIRO)

8.1 The Director of People & Communications is responsible for ensuring that a robust incident reporting process is in place and will:

- work with colleagues to ensure an integrated approach to patient safety and embed a risk management culture throughout HEE;
- develop a culture of learning lessons from incidents sharing the lessons learned and changing practice as required;
- maintain the Serious Incidents and incident reporting systems;
- be responsible for consistently implementing the organisational arrangements for incident reporting throughout the organisation;
- ensure that all incidents are investigated appropriately in accordance with their severity and are signed off as completed;
- report any patient-centered incident to NHS Improvement via their online reporting form National Patient Safety Agency;
- collate data quantitatively and qualitatively for reporting to the Integrated Governance Committee at appropriate intervals, including Learning from Incidents;
- offer advice to managers in the investigation of incidents; and
- offer support to staff during the investigation of incidents.

8.2 HEE's Director of People & Communications, is the appointed Senior Information Risk Owner (SIRO) for HEE.

9. Caldicott Guardian

9.1 The Caldicott Guardian is a senior person responsible for protecting the confidentiality of service-user information and enabling appropriate information-sharing and championing Caldicott at the board.

9.2 HEE's Executive Director of Education and Quality & National Medical Director, is the appointed Caldicott Guardian for HEE.

10. Regional Directors

10.1 Regional Directors will usually be the investigating manager (see below) and should acknowledge, investigate and provide feedback to staff about incidents that have been reported. They are also responsible for ensuring that:

- all staff receive relevant training;

- ensuring that reporting to RIDDOR is undertaken where necessary as per Incident Reporting including RIDDOR (Health & Safety) SOP
- arrangements are put in place to support staff who are involved in an incident (this should not be the lead investigator);
- where the investigation overlaps with other procedures, e.g. complaints, disciplinary these are dealt with under a separate investigation process;
- where potentially fraudulent activity is identified as part of the investigation this is reported to the Local Counter Fraud Specialist or through the NHS Fraud and Corruption Reporting Line (0800 028 40 60); and
- learning is shared in line with the Learning from Experience Policy.

Regional Directors are responsible for reviewing the electronic incident forms and processing them for final approval.

11. Associated Documentation

11.1 Information Asset Owners (IAOs) are senior members of staff at manager level responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks; this should be done through Corestream. Data Custodians should ensure that:

- All IG incidents are reported to the Information Governance Lead, their IAO/line manager within 24 hours of becoming aware;
- Cyber incidents are reported to both the IG Team and IT as soon as possible but within 12 hours of becoming aware;
- they consult with their IAOs on incident management procedures;
- they familiarise themselves with the IG and cyber s ecurity SIRI process;
- recognise actual/potential IG or cyber security incidents and take steps to mitigate the risks;
- staff in their directorate/departments follow HEEs procedures and guidance documents;
- Staff Guideline on Identifying and Reporting IG or cyber security incidents can be found within the Information Governance and Cyber Security Incident Management and Reporting Procedures.

12. Staff

12.1 Staff are responsible for highlighting any risks or issues to the IG Team, which could warrant further investigation. Any member of staff can complete an incident reporting form.

12.2 Electronic incident forms are accessible via HEE's intranet pages. Paper versions are available from the IG Team in the event that the electronic version is inaccessible.

12.3 All staff should be fully open and co-operative with any investigation process.

12.4 Staff are responsible for reporting, completing and grading incidents as soon as possible after the incident is identified but no later than 12 hours following a cyber incident and 24 hours following an IG incident. If the member of staff is unable for any reason to complete the form themselves, it is acceptable for a colleague to do so on their behalf.

13. Independent Contractors

13.1 Independent Contractors are required to report all HEE related incidents to HEE.

14. Definition of Terms

14.1 There are three main types of incidents which are defined below:

a) Near Miss (Prevented Incident)

14.2 A near miss is an incident that had the potential to cause harm, loss or injury but was prevented. These include cyber, clinical and non-clinical incidents that did not lead to harm, loss or injury, disclosure or misuse of confidential data but had the potential to do so.

14.3 A near miss incident should be distinguished from a 'no harm' incident, which is where the incident happened, but no harm resulted (for example, out of date medicine administered, but the patient suffered no ill effects).

b) Incident

14.4 An incident is any injury, loss, damage or abuse to staff, service user, visitor, external contractor, student, volunteer or other person, or to property/equipment.

14.5 Incidents may be caused by any of the following:

- human error;
- systems failure;
- a combination of several small mistakes occurring at the same time or
- a cyber-attack

c) Serious Incidents (SI)

14.6 An SI is an incident where a patient, member of staff or a member of the public has suffered serious injury, major permanent harm or unexpected death on health service premises or other premises where health care is provided.

14.7 An SI can also be an occasion where actions of health service staff are likely to cause significant public concern.

14.8 HEE has a separate Serious Incident procedure for the management of serious incidents.

14.9 The definition of an IG incident is “Any incident involving the actual or potential loss of personal information and/or breaches of confidentiality that could lead to identity fraud or have other significant impact on individuals should be considered as serious”.

14.10 IG and cyber security Serious Incidents Requiring Investigation (SIRIs) are incidents which involve actual or potential failure to meet the requirements of the GDPR/Data Protection Act 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, inappropriate invasion of people’s privacy and personal data breaches which could lead to identity fraud or have other significant impact on individuals. This definition applies irrespective of the media involved and includes both electronic media and paper records.

15. Incident Management Structure, Accountabilities & Responsibilities

15.1 HEE has an organisational structure in place to help manage and implement risk management systems. This is described below.

15.2 The Audit Committee and the reporting structures of HEE are designed to work together to ensure a concerted and integrated approach to the management of risk. The primary purpose of risk management is to enable the organisation as a whole and individuals to deal competently with all key risks either clinical or non-clinical.

15.3 Annex A sets out the process for Information Governance Incident Processing.

15.4 The Incident Reporting including RIDDOR (Health & Safety) SOP sets out the process for Health & Safety related incident reporting including incident reporting as required under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2015 (RIDDOR).

a) The Board

15.5 The Board has ultimate responsibility for the management of risk and for agreeing the annual Statement of Internal Control. It receives reports and assurance from the governance committee on the quality and safety of services and assurances of the effectiveness of risk reduction strategies.

15.6 The Board has delegated its powers to the Executive Team to identify and manage risks on its behalf.

b) Audit Committee

15.7 The organisation's Audit Committee assists the Board by carrying out a review of the effectiveness of the management of risk activities, providing assurance and an independent overview on risk management.

c) Counter Fraud in the NHS

15.8 A Counter-Fraud and Anti-Bribery Policy is in place and is available to staff via the intranet.

16. Training needs Analysis

16.1 HEE recognises that learning from incidents is vital to prevent recurrence. IG training or retraining will be provided to affected staff members when necessary.

17. Monitoring Compliance with and the Effectiveness of Procedural Documents

17.1 The final review of all electronic incident forms will ensure that investigation and feedback to staff has been carried out.

17.2 Quarterly reports on incident numbers, trends and themes will be provided to the Audit Committee together with an Annual Report

18. References

18.1 The following guidance and legislation has been used in the development of this policy:

i. General Data Protection Regulation

ii. Data Protection Bill/Act

iii. Seven Steps to Patient Safety – NPSA Doing Less Harm – DoH and NPSA, 2001 An Organisation with a Memory – DoH, 2000

iv. Building a Safer NHS for Patients – Implementing an Organisation with a Memory - DoH, 2001

v. Design for Patient Safety – DoH 2005

vi. Safety First: A report for patients, clinicians and healthcare managers – DoH 2006

vii. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2015 (RIDDOR) – Health & Safety Executive (HSE)

viii. Procedure for the Management of Serious Untoward Incidents (SUIs) – NHS Yorkshire and the Humber

ix. Being Open When Patients are Harmed – NPSA 2005

x. NHSLA Risk Management Standard 5 – Learning from Experience Standards for Better Health first (safety) and third (governance) domains – Healthcare Commission

xi. Health & Safety at Work Act 1974 – Health & Safety Executive (HSE)

xii. Management of Health & Safety at Work Regulations 1999 – Health & Safety Executive (HSE)

19. Associated Documentation

- Acceptable Use of Mobile Devices and ICT
- Records Management Policy
- Counter-Fraud and Anti-Bribery Policy
- Raising Concerns at Work (Whistleblowing) Policy
- Health & Safety Policy Incident Reporting including RIDDOR (Health & Safety) SOP Risk Management Policy
- Business Continuity Policy
- Information Security Policy
- Incident Management Procedure.
- Guide to the Notification of Data Security and Protection Incidents (NHS Digital)

Annex A: Information Governance Incident Processing

1. Introduction

1. Some incidents may be classified as Information Governance Serious Incident Requiring Investigation (SIRI). An IG SIRI is any incident which involves actual or potential failure to meet the requirements of the GDPR/Data Protection Act and/or the Common Law of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches, inappropriate invasion of people's privacy and personal data breaches which could lead to identity fraud or have other significant impact on individuals. This definition applies irrespective of the media involved and includes both electronic media and paper records relating to staff and service users.

2. Since June 2013 all NHS organisations that process health and adult social care personal data must use the Data Security and Protection Toolkit (previously the IG Toolkit) Incident Reporting Tool to report level 2 IG Serious Incidents Requiring Investigation (SIRIs) to the Department of Health and Social Care (DHSC), NHS England and the Information Commissioner's Office (ICO). IG SIRI functionality was extended in early 2015 to enable capture of cyber related incidents.

3. A cyber-related incident is anything that could compromise 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.

4. Please refer to NHS Digital's *'Guide to the Notification of Data Security and Protection* Incidents' document for further information

5. Procedures have been developed to document the approach taken by HEE in processing IG incidents under the new guidelines. Please refer to HEEs incident management procedure and to the Information Governance & Cyber Security Incident Management and Reporting Procedures documents.

2. Duties

6. **Staff:** Will continue to report IG-related incidents to the IG Team using the standard documentation within HEE's incident management procedure document identified above.

7. **Head of Corporate Affairs:** Will receive copies of IG related incident reports from Information Governance and process them under the Local Working Instructions set out in (3) below.

8. **Information Governance Lead / Head of Public and Parliamentary Accountability:** Will provide expert input to assist with the grading of IG-related incidents and deputise for the Head of Corporate Affairs under the Local Working Instructions set out in (3) below when required.

9. **Medical Director / Director of People & Communications (as SIRO) and the Information Governance Steering Group (IGSG):** Will provide support to the IG Lead as required, including:

   - Input on incident grading
   - Post-incident action planning & communication
   - Input on recurrence prevention measures
   - Board-level awareness of SIRI-grade incidents and low-level incident trends

3. Local working instructions all incidents

11. The Information Governance Team will receive copies of all IG-related incident reports.

12. The Information Governance Lead will assess the report and consider whether it contains all information required to grade the incident.

13. Any deficiencies / omissions in the report will be followed up by the Information Governance Team with the reporting staff / manager named in the report.

14. The incident will be graded under the IG Incident grading methodology from the Guidelines.

15. The incident will be summarised in the incident spreadsheet for presentation to the bi-monthly IGSG.

4. Level 2 (and higher) SIRI Incidents

16. On grading any incident at level 2 or higher, the Information Governance Lead will escalate the incident as follows:

- Head of Corporate Affairs
- Data Protection Officer(s)
- Director of People & Communications (as SIRO) – all incidents
- Medical Director – trainee / service user related incidents
- Chief Executive – all incidents

17. Level 2 or higher incidents will be filed within the IG Incident Reporting Database and submitted to the ICO via the Data Security and Protection toolkit.

18. The incident will be updated internally as required as any further investigation or actions are progressed.

19. The incident will be "closed" when the ICO notify HEE that all appropriate actions have occurred and no further investigation is necessary.

20. The Data Protection Officer(s) will be first point of contact for external agencies (ICO etc.) for incident escalation.