Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

POLICY REFERENCE NUMBER:	CPG50d
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	3 year review; minor changes
AUTHOR:	[redacted] Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub-Committee. Quality Committee.
IMPLEMENTATION DATE	June 2019
AMENDMENT DATE(S)	October 2019 (ID no. Change); Sept 2021
LAST REVIEW DATE	September 2021
NEXT REVIEW DATE	September 2024
APPROVAL BY IGSSC	August 2021
RATIFICATION BY QUALITY COMMITTEE	September 2021
COPYRIGHT	

PROCEDURE SUMMARY

The purpose of this policy and its associated procedural guidelines is to establish the governance arrangements and responsibilities for information security, with the intention to promote and build a level of consistency across the Essex Partnership University NHS Foundation Trust ('the Trust') to safeguard information, ensuring all Trust staff are aware of their individual responsibilities.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate. Also through Trust Datix Reporting and
Compliance with the IG Toolkit submission

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is The Executive Chief Finance & Resources Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLESAE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

1. INTRODUCTION

1.1 This procedure is a Trust-wide document and applies to all staff.

1.2 It should be read in conjunction with the Trust's Information Security Incident Management Procedure & Risk Management Policy.

1.3 The Trust is committed to the promotion of a learning and fair blame culture, where staff understand the need to report all incidents.

1.4 Throughout this policy an incident refers to all accidents, incidents and near misses.

1.5 All Trust staff should report any incident including near misses, incidents and safety issues. The Trust assures staff through processes such as the 'whistleblowing policy' (Raising Concerns (Whistleblowing Policy, CP53) that the information they share will be treated with respect and acted upon appropriately to improve the safety and quality of the service we provide for our patient/service users and the safety and quality of the work environment for staff and visitors.

1.6 In line with the Duty of Candour Requirements (2014) the Trust also has a Being Open policy (CP36) to ensure that when mistakes are made patients/relatives/carers receive an acknowledgement, apology and a truthful and clear explanation as soon as a patient safety incident has occurred.

Saying sorry is not an admission of liability it is the right thing to do.

1.7 Communication with patients, carers and the public must be fully documented.

2. PURPOSE

2.1 The aim of the procedure is to provide:

- Staff with clear information on how to report incidents via the Datix electronic online incident reporting system
- An outline of the management of incident reporting in the Trust and to external agencies/stakeholders
- The Trust's approach on the investigation, analysis, and learning and improvement from incidents
- A procedure for the investigation of reported as major or catastrophic harm including SIRIs (Serious incidents requiring investigation) Near Miss and Never Events.

- Procedures for investigating specific generic incident types

2.2 The purpose of the procedure is to outline the arrangements for identifying, managing, investigating and reporting accidents, incidents and near misses within the Trust.

2.3 This procedure covers reporting and recording procedures for managers, employees and non-employees.

2.4 The reporting of all incidents, prevented incidents (near-misses) is designed to ensure the following:

- A culture of openness in reporting incidents or prevented incidents (near misses);
- Prompt and precise gathering of information;
- Prompt communication with staff and where appropriate the media;
- Minimisation of distress to those affected by an incident;
- Identification of patterns and trends in the occurrence of incidents and prevented incidents (near-misses);
- Minimise, so far as is reasonably practicable, future risk by taking prompt and appropriate preventive action and on - going monitoring;
- Early warning of potential litigation and cost impact;
- Managers are able to review existing safety procedures;
- Fulfilment of the Trust's legal duties under statutory regulations.

3. DEFINITIONS

For the purposes of this procedure the following definitions apply:

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy

- Other significant economic or social disadvantage to individuals

4. ROLES AND RESPONSIBILITIES

Duties within the Organisation

4.1 Executive and Senior Team

Executives and senior managers are responsible for the health and safety of employees and visitors in their specified location/areas. As such they have the primary responsibility for ensuring this procedure is fully implemented in their area.

4.2 Managers

Managers are responsible for implementing the policy by:

- Ensuring that all staff are up to date with Information Governance training aware of the procedures;
- Support & encourage staff in the reporting of accidents and near misses;
- Ensuring appropriate and timely reporting of incidents;
- Supporting the reporting process of reviewing and investigating local Incidents;
- Taking local remedial and preventative action;

4.3 Employees

All employees are responsible for:

- Reporting any incident/accident/near miss in line with this procedure;
- Adhering to the employee requirements of the Health & Safety at Work Act 1974;
- Provision of reports as requested as part of an investigation.
- Undertake the annual mandatory training

5. REPORTING PROCESS

5.1 All incidents (including near misses and out of hours) must be reported using the Trust reporting electronic system called Datix. Datix provides a systematic process which enables incidents to be reported and then investigated.

5.2 All incidents should be reported as soon as the staff member is able, ideally within 24 hours ensuring patient safety remains a priority.

Do not delay reporting if some information is unavailable; this can be added later.

5.3 All staff have access to Datix. Datix is found on the Staff Input pages.

5.4 For all patient safety incidents reported as moderate, major or catastrophic harm, the Trust has a 'Duty of Candour' to offer an apology to the patient or relevant person.

5.5 Datix electronic incident reporting forms must be completed as comprehensively as possible and should give a clear factual and objective account of what happened i.e. who, why, what, where and how. They should also include information on the immediate actions taken following the incident together with any actions planned or taken to prevent a reoccurrence.

5.6 Incident forms must contain factual information and exclude personal opinion or assumption.

5.7 If an incident has involved a patient, clinical staff must also record what happened and any action taken in the patient's medical records.

5.8 Notifiable breaches are those that are likely to result in a high risk to the rights and freedoms of the individual (data subject). The scoring matrix used in incident reporting has been designed to identify those breaches that meet the threshold for notification.

5.9 However, there are also a number of breaches of security that are also reportable under Network and Information Systems Regulations 2018 which must also be recorded on the Data Security & Protection Tool even if organisations believe they are not notifiable under the General Data Protection Regulation (GDPR).

5.10 The GDPR Article 33 requires reporting of a breach within 72 hours. The 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised.

5.11 This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts.

5.12 Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

5.13 Local records required for an incident notified to the ICO

A local file, which may be requested by the Information Commissioner, must be maintained which must contain the following sections;

- the facts relating to the breach.
- its effects.
- the remedial action taken.

The local file of the investigation for the Trust is the Datix System.

The Datix reporting tool will forward to the appropriate organisation indicated in the scoring matrix. The organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident may be shared onward.

5.14 ICO

Any incident graded as notifiable, will be reported by the Information Governance team through the Data Security & Protection Toolkit (DSPT) to the ICO and will result in the incident being forwarded to the Information Commissioner. The Information Commissioner will then decide if any action is necessary.

5.15 Department of Health and Social Care

Any incident that scores more than a 3 on both axes on the scale will be immediately reported to the Department of Health and Social Care so that the relevant officials can be made aware of any breach that is likely to have an impact on service users and the running of the health and social care sector.

5.16 NHS England

Any incident that scores more than a 3 on both axes on the scale will be reported to NHS England to help inform operational delivery and future commissioning arrangements.

5.17 NHS Digital

As well as hosting the Data Security and Protection Incident Reporting Tool the information contained within reported breaches may be used as intelligence especially when there could be an effect on the system and services it provides which are relied upon across the sector.

6. STAFF, PATIENTS AND CARERS

Involvement in an incident can undermine confidence for patients, carers and families. The member of staff who is nominated to inform the patient/relative/carer about the incident should offer all necessary support. [Trust's Being Open Policy]

Staff who are responsible or involved in an incident should receive feedback, from their manager, regarding any investigation, including recommendations and actions taken to reduce the risk of reoccurrence.

7. UNDERTAKING AN INVESTIGATION

7.1 The individual to whom the incident has been assigned (the handler) should ensure an investigation occurs.

The Handler must record the details of the investigation and the outcome on Datix.

This person remains responsible for ensuring that all relevant information is documented on the online Datix investigation form and that sufficient information is provided on the feedback section of the form.

7.2 Investigations should be carried out in such a way as to promote a non-threatening environment, with emphasis on learning from the incident, rather than apportioning blame.

7.3 Confidentiality of all individuals concerned should be protected as far as possible throughout the investigation, ensuring all written documentation is stored in a secure environment.

7.4 An investigation must be carried out as soon as possible after an incident has occurred.

A good starting point is to collate and gather initial evidence, for example by speaking with staff, visiting the scene, collecting any relevant documentation and securing any evidence.

Additional information that may need to be obtained includes for example, training records, risk assessments, staff duty rotas, policies and procedures, etc.

7.5 All details regarding the incident must be documented and all staff should be reminded that any records kept may be disclosable.

The information gathered should be reviewed, a chronology of events determined and the following key pieces of information established:

- What happened? Where? Check exact locations and times.
- Who was involved?
- Who was affected?
- Has it happened before?
- What impact has the incident had?
- Were there any witnesses?
- What action has already been taken? By who?
- Who has been informed?
- Has an incident form been submitted?
- Do written statements need to be obtained?
- Who else needs to know? e.g. external agencies/stakeholders and/or internal departments/key individuals
- What else needs to be done?

7.6 Some investigations will require staff to provide written statements of their involvement. This can best be achieved by contacting the individual and making a record of their description of events.

8. MISCONDUCT

8.1 Where an incident upon investigation, identifies that an individual acted in a manner, which knowingly placed themselves and others at significant risk or if misconduct or fraudulent behaviour is identified, disciplinary action may follow.

8.2 If a member of staff knowingly fails to report an incident it will be in breach of this procedure.

8.3 Where an individual staff member repeatedly make the same mistakes, or are persistently closely involved with incidents and fail to learn from the support and training provided by the organisation, then the Trust's Capability policy and procedures will be followed.

9. GRADING INCIDENTS

9.1 The severity of an incident or consequence, along with the likelihood of reoccurrence is applied to the incident which could involve staff, patients and others to establish a grade e.g. near miss, negligible, minor, moderate, major, and catastrophic.

A scoring matrix (below) is used by the Information Governance team to help identify the appropriate score for an incident.

All incidents including near misses are graded; however a near miss will be graded in relation to the potential harm as opposed to the actual harm.

9.2 Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of special categories/vulnerable groups it must be assessed as at least:

- A Likelihood of 'Not likely or incident involved vulnerable groups (where no adverse effect occurred)' Not Likely on the grid.

And

- A Severity of 'Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred'. Minor on the grid.

So even where an incident involves special categories/vulnerable groups, on the breach assessment grid above, it would be a minimum of 4 and so would not be always be reported to the ICO. It would be reported to the ICO if the Likelihood of harm is assessed as at least 'Likely'.

9.3 Special Categories of personal data

For clarity special categories under GDPR are:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- the processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation

9.4 For clarity special categories under GDPR not listed above include:

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 (where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual)
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

9.5 Assessing risk to the rights and freedoms of a data subject (likelihood)
The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Depending on the outcome of the scoring matrix contained in this procedure the risk may be high risk and be significant enough to notify to the ICO. If there is any doubt that a breach is significant enough for notification it is always best to notify.

9.6 Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than "grey breaches" being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.

					DHSC & ICO		
Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
					ICO		
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

10. ANALYSIS AND FEEDBACK OF COLLATED INCIDENT REPORTS

10.1 The Trust recognises the importance of learning. In order to ensure an aggregated review of incidents and the opportunity to learn wider lessons, the Associate Director of Electronic Systems and Information Governance will be responsible for co-coordinating a monthly report to the Learning Oversight sub-committee (LOSC) meeting.

10.2 Escalating concerns/issues identified through analysis

The LOSC meeting will escalate any unresolved issues to the Trust Quality Committee. The Quality Committee will receive assurance that work streams are progressing.

10.3 Incidents should be discussed at Ward/Department meetings. Amber and Red incidents will be discussed at the Information Governance Steering Group / Quality Board. The identified actions and lessons learned are shared Trustwide in the staff Wednesday Weekly Communication Articles.

END