Trust Standard Operating Procedure

NHS University Hospitals Plymouth NHS Trust

Information Governance Incident Handling SOP

Issue Date	Review Date	Version
June 2018	June 2023	5

Purpose

The purpose of this procedure is to ensure that any information governance serious incidents that require investigating (IG SIRI) are handled appropriately and that the guidance issued by NHS Digital and the Trust Incident Management Policy are followed.

Who should read this document?

This document is relevant to all staff who work for, or on behalf of Plymouth Hospitals NHS Trust.

Key Messages

When an IG incident occurs you must:

- Ensure continuation of patient care
- Secure the data
- Record on Datix
- Tell the IG team
- Tell the line manager
- Give a Verbal/Written apology

Core accountabilities	
Owner	Information Governance Support Manager
Review	Caldicott and Information Governance Assurance Committee
Ratification	Head of Information Governance on behalf of Director of Corporate Business
Dissemination	Information Governance Support Manager
Compliance	Information Governance Support Manager

Links to other policies and procedures

Incident Management Policy
Incident Management Procedure
Performance and Conduct Policy

Version History

V1.1	March 2010	Initial Draft
V2	April 2014	Document review completed and transferred to SOP template
V2.1	December 2014	Update to Appendix 1
V3	June 2015	Reviewed in light of changes to the Trust's Incident Management Policy, the NHS Digital checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation and the Serious Incident Framework by NHS England

V3.1	August 2016	Minor amendments to change of name for HSCIC to NHS Digital
V4	November 2017	Reviewed in line with Data Protection Reform due to May 2018
V5	June 2018	Reviewed in line with new incident scoring guidance, 'Guide to the Notification of Data Security and Protection Incidents'

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents on StaffNET. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

Standard Operating Procedure (SOP)

Information Governance Incident Management

1 Introduction

This document sets out the procedure for all University Hospitals Plymouth NHS Trust staff to follow in the event of a breach of Data Protection Legislation in line with the *'Guide to the Notification of Data Security and Protection Incidents',* NHS Digital, July, 2018.

Processing personal information must comply with Data Protection Legislation:

- UK Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- Common Law of Confidentiality

2 Definitions

Personal Information

Factual information or expressions of opinion, which relate to a living individual who can be identified from that information, or in conjunction with any other information coming into the possession of the holder of that data – this also includes any indication of the intention of any person in respect of that individual.

Serious Incident Requiring Investigation

An incident involving actual or potential failure to meet Data Protection Legislation or the Common Law Duty of Confidentiality.

Confidentiality

Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Data Subject

The subject of the personal data.

3 Regulatory Background

Data Protection Legislation

The following sets out the way organisations should process personal data of living individuals:

- EU General Data Protection Regulation (GDPR)

- UK Data Protection Act 2018.

Common Law Duty of Confidentiality

Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Guide to the Notification of Data Security and Protection Incidents, NHS Digital, July, 2018.

4 Key Duties

The key duties are to:

- Ensure continuity of patient care
- Contain and recover personal data
- Investigate and assess ongoing risk
- Notify the data subject of the breach and issue an apology
- Evaluate the incident and produce investigation findings
- Report any 'IG Reportable Incidents' on the NHS Digital Incident Reporting Tool located on the Data Security and Protection Toolkit and to the relevant Clinical Commissioning Group via STEIS

5 Procedure to Follow

Information Governance Incident

All information governance incidents should be reported by the staff member involved in, affected by or witnessing the event on the Trust's incident reporting system, Datix. The Information Governance Team should be informed so that action can be immediately taken to contain the incident and preserve evidence.

An immediate response is imperative to ensure that patients are not affected and that the incident does not impede on healthcare. For example, in cases where hospital letters have been received by the incorrect recipient, it is essential that the correct patient receives a replacement letter to ensure care continuity.

Recovering data/containing incident

The recovery of personal information that is disclosed in error is necessary to ensure that further dissemination does not occur.

<u>Incidents where paper has been given/sent to the wrong patient:</u>

In instances where the Trust are informed of information being received in error, the cost of returning the data should be met by the Trust in the form of supplying a stamped addressed envelope.

All staff have the responsibility to maintain patient confidentiality and should pick up personal information if found. If it is not possible to hand in to a Line Manager, the Information Governance Team can be contacted to discuss collection.

For information found and handed over in person, staff must;

- Thank the person(s) for handing in the information
- Ascertain incident details and report this on Datix
- Issue an apology
- Inform the IG team and provide them with the incident reference number

It is also recommended that where possible, information is scanned and emailed to the IG team using the secure multi-function printers and the original placed in the confidential waste.

Incidents where information has been emailed to the wrong patient:

If the information has been disclosed via email to someone it shouldn't have been then the sender of the email must recall the email immediately. To recall an email:

- Double click on the email in the sender's Sent Items folder
- Click on the Actions button along the top of the screen and select Recall This Message
- Select Delete unread copies of this message and click OK.

Be aware, the recall function does not work if the email has been read by the person who received the email in error. This means in cases where the Trust is contacted by someone who states that they have received an email from the Trust in error we will not be able to recall the email. In this situation staff must:

- Thank the person(s) for making the Trust aware
- Ask them to delete the email from their mailbox
- Ascertain incident details and report this on Datix
- Issue an apology
- Forward a copy of the email disclosed in error to the IG Team and provide them with the incident reference number

Taking responsibility and disciplinary action

All staff who have contributed to a serious information governance breach may be subject to informal/formal action in accordance with the Performance and Conduct Policy.

Advice should be sought from Human Resources/Medical HR.

Issuing an apology

The Service Line responsible for the breach must issue either a verbal or written apology to the data subject(s).

In the majority of cases it is standard practice for a data subject(s) to be informed when their data has been wrongfully disclosed. If it is not in the patient's best interest to be informed and the healthcare professional responsible for their care has agreed this decision, it should be clearly documented, including any action to inform the data subject at a later date.

Onward reporting

All incidents are scored for severity by the IG team using the scoring matrix below published in the, *'Guide to the Notification of Data Security and Protection Incidents'* written by NHS Digital, June 2018. Those that score in the coloured sections of the matrix are potential IG Reportable Incidents and must be escalated to the Data Protection Officer (DPO), Senior Information Risk Owner (SIRO) and Caldicott Guardian for confirmation of the severity level.

IG Incident Scoring Matrix

Incident Ref:	
Name of Scorer:	

Please score this incident for severity by putting an x in the relevant box.

For example if the incident has had no impact and the likelihood of harm has not occurred mark the box numbered 1 with an x:

No Impact	1
	x
	Not Occurred

Impact	**Catastrophic**	**5**	5	10	15	20	25
	Serious	**4**	4	8	12	16	20
	Adverse	**3**	3	6	9	12	15
	Minor	**2**	2	4	6	8	10
	No Impact	**1**	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
			Not Occurred	**Not Likely**	**Likely**	**Highly Likely**	**Occurred**
			Likelihood Harm Has Occurred				

Key

	Reportable to the ICO Incident
	Reportable to the ICO Incident, DoH will also be notified

All IG Reportable Incidents should be reported using the NHS Digital Incident Reporting Tool on the Data Security and Protection Toolkit within 72 hours of the breach occurring. The tool will automatically notify the Information Commissioner's Office (ICO) of the incident and in some cases where the incident severity is very high, the Department of Health will also be notified. As soon as an incident has been reviewed by the ICO and marked as closed it will be published quarterly by NHS Digital.

IG Reportable Incidents should also be reported via STEIS to inform North, East and West (NEW) Devon Clinical Commissioning Group (CCG) so that they can review the incident and liaise with the Trust. A root cause analysis investigation must be conducted. Please see the Incident Management Policy and the Incident Management Procedure for Serious Incidents for more details on the reporting process to the relevant CCG.

All IG incidents are reported quarterly to the Caldicott and Information Governance Assurance Committee. Key facts and areas of concern are also reported to the Trust Board by the Senior Information Risk Owner.

The Information Governance Team are required to produce annual figures for the Trust Annual report which is published on the Trust external facing website.

Please see process map (Appendix 1) for handling IG Incidents.

6 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Director of Corporate Business.

Non-significant amendments to this document may be made, under delegated authority from the Director of Corporate Business, by the nominated author. These must be ratified by the Director of Corporate Business and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

7 Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Director of Corporate Business and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

8 Monitoring and Assurance

Incidents will be managed in line with the NHS Digital *'Guide to the Notification of Data Security and Protection Incidents'* and the Trust Incident Management Policy.

Staff that breach confidentiality may be subject to disciplinary action in line with the Trust Performance and Conduct Policy.

All incidents and Root Cause Analysis reports will be reported at the Caldicott and Information Governance Assurance Committee.

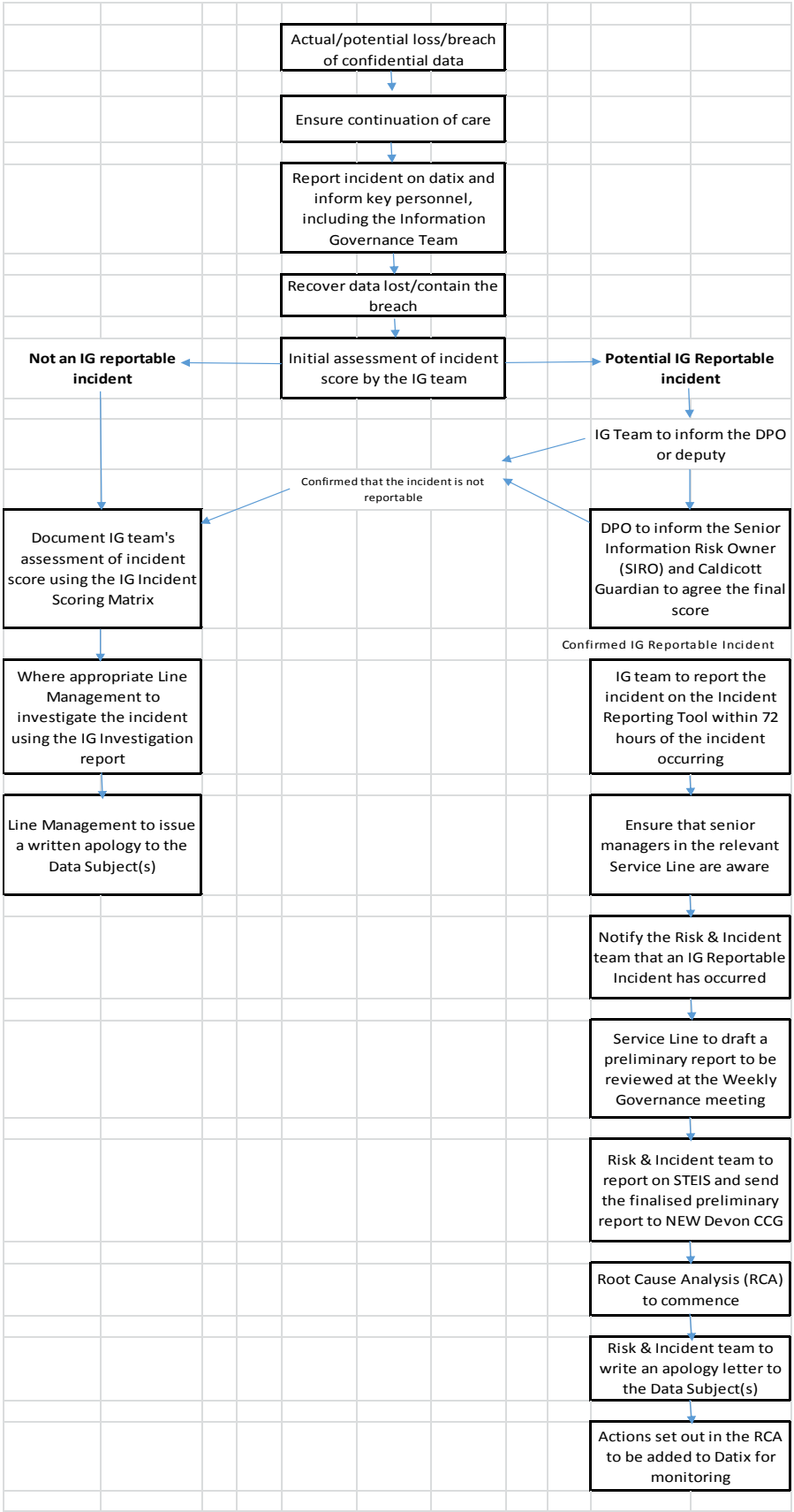
9 Reference Material

Guide to the Notification of Data Security and Protection Incidents, NHS Digital (June 2018)

Serious Incident Framework, NHS England (March 2015)

Incident Reporting Tool, Data Security and Protection Toolkit, NHS Digital (July 2018)

Information Governance Incident Procedure to Follow | Appendix 1



Information Governance Incident Scoring Matrix — Appendix 2

IG Incident Scoring Matrix

Incident Ref:	
Name of Scorer:	

Please score this incident for severity by putting an x in the relevant box.

For example if the incident has had no impact and the likelihood of harm has not occurred mark the box numbered 1 with an x:

No Impact	1
	x
	Not Occurred

Impact	**Catastrophic**	**5**	5	10	15	20	25
	Serious	**4**	4	8	12	16	20
	Adverse	**3**	3	6	9	12	15
	Minor	**2**	2	4	6	8	10
	No Impact	**1**	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
			Not Occurred	**Not Likely**	**Likely**	**Highly Likely**	**Occurred**
			Likelihood Harm Has Occurred				

Key

	Reportable to the ICO Incident
	Reportable to the ICO Incident, DoH will also be notified

University Hospitals Plymouth NHS Trust

Unit/Department Name
University Hospitals Plymouth NHS Trust
Derriford Road
Crownhill
Plymouth
PL6 8DH

Tel: 01752 202082
www.plymouthhospitals.nhs.uk

Dear <insert name>

Introduction/Purpose of letter

The reason why the letter has been produced, including apology.

Description of Events/Incident Overview

Description of the incident

Immediate remedial action taken

Root Causes

The reason(s) why this incident occurred.

Lessons Learned

Measures put into place to prevent this incident from occurring again.

Details of who to contact/further action is required

Details of Complaints Department/Service Line Manager.

<<Insert signature>>