NHS
West Lancashire
Clinical Commissioning Group

Standard Operating Procedure

Information Governance Breach Reporting

West Lancashire CCG

Version 1

February 2021

With you.
For you.

Item		Responsible
1	Purpose	Guidance
2	Document Purpose	Procedures
3	Document Name	Standard Operating Procedure for the reporting and logging of data security and protection breaches
4	Author	Information Governance Team, MLCSU
5	Version	1.0
6	Publication Date	19th February 2021
7	Review Date	1 year from approval
8	Target Audience	All staff within West Lancashire CCG
9	Cross Reference	Information Governance Data Security and Protection Policy and IG Handbook
10	Superseded Document	N/A
11	Approved by	Governing Body 16th February 2021
12	Contact Details	MLCSU IG Team Email: mlcsu.ig@nhs.net Tel: 01782 872648

Version	
V1.0	Draft new local breach reporting SOP

Introduction

This Standing Operating Procedure (SOP) sets out what staff should do when they become aware of a data security and protection breach.

It is important that information remains safe, secure, and confidential at all times.

All staff are encouraged to report all breaches via the Breach Reporting Form as soon as is possible following the identification of the breach.

NOTE: Although the general guidance is that breaches should be reported within 72 hours, if the breach is highly severe, it will require reporting within 24 hours to meet Department of Health timescales. Therefore, we will base reporting timescales on 24 hours rather than 72.

All health and social care organisations are to use the reporting tool accessed via the Data Security and Protection Toolkit to report data breaches. This reporting will be undertaken by the CSU IG Team.

What is a Data Breach?

Breach of Confidentiality - A data breach, as defined under GDPR/DPA18, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, **personal data** transmitted, stored, or otherwise processed.

(Personal data is defined as: 'any information relating to an identified or identifiable individual)'

Breach of Process – Where a process has not been followed but no identifiable information has been disclosure.

Reporting Process

1. Inform the **CSU IG Team**, and **line-manager** within 24 hours of becoming aware of a near miss, breach or potential breach.

   IG Team

   Email: mlcsu.ig@nhs.net

   Tel: 01782 872648

2. CSU IG Team to contact the reporter at their earliest opportunity to obtain the information required for the completion of the Reporting Form (Appendix A – Reporting Form). Some of the questions within the Reporting Form are subjective depending on the breach itself. Some of the questions may not be relevant depending on some of the other answers**.**

3. Reporter to return the answers to the **CSU IG Team**, copying in their **Line-Manager** within 24 hours
4. **CSU IG Team** to log the breach, this will generate a CMS number which is to be used in all further correspondence
5. **CSU IG Team** to inform the **reporter**, and the **line-manager** of any immediate action needed to be taken
6. **CSU IG Team** to inform the SIRO of the breach
7. **CSU IG Team** to report the breach on the DSP Toolkit once authorised by the SIRO

NOTE: The DSP Toolkit will establish if the breach is reportable to the Information Commissioner Office (ICO) and RCA is needed

If the breach is non-reportable, an RCA is unlikely to be needed. If the breach is reportable, the RCA must be sufficient to meet ICO requirements.

Investigation Process

NOTE: The Investigation process is to establish what happened and what can immediately be done to mitigate the consequences of the breach.

- **The CSU IG Team** will undertake an investigation alongside the **CCG**

Route Cause Analysis (RCA)

NOTE: The Root Cause Analysis (RCA) process is to establish what caused the breach to happen and develop actions to prevent similar breaches occurring again.

1. CSU IG Team to discuss with the line-manager of the team, and the IG Lead for the CCG, who should be appointed as the lead for the RCA
2. The CSU IG Team to liaise with the RCA lead as to how to establish the root cause of the breach (Appendix B – RCA Guidance)
3. Once completed, the CSU IG team to develop a list of recommendations which will be send to the SIRO, DPO, CG, IG Lead, IG BPs and line-
4. Line-manager/RCA Lead to present their actions and outcomes to the IG steering group
5. Caldicott Guardian to work with CSU IG Team to determine whether the data subject should be informed where the breach involves identifiable information

The RCA should include:

1. Breach description
2. Pre-investigation risk assessment
3. Background and context of the breach
4. Information and evidence gathered
5. Report Limitations (as appropriate)
6. Chronology of events

RCA DOCUMENTS

Date	Event

Contributory factors

What happened?	Root Cause – Why did it happen?	Lessons Learnt	Action to implement lessons learnt

Recommendations/Action Plan (incorporates plan for lessons learnt)

Recommendations	Action	Person Responsible	Deadline Date

Appendices

Appendix A – Reporting Form

Breach form.docx

Appendix B – RCA Guidance

Root Cause Analysis guidance.p

Get to know us or get in touch

mlcsu

Midlands and Lancashire Commissioning Support Unit

midlandsandlancashirecsu.nhs.uk