NHS
Cheshire and Merseyside

Standard Operating Procedure: Information Governance Breach Reporting

NHS Cheshire and Merseyside ICB

Document Owner: MLCSU IG Team	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

Introduction

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

Breach Reporting Process

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

   CSU 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 following information (Appendix A – Reporting Form):

   The questions are all 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 and line-manager within 24 hours
4. CSU IG Team to log the breach, this will generate a Sostenuto Reference Number which is to be used in all further correspondence
5. CSU IG Team to inform the reporter and their 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 if authorised by the SIRO

NOTE: The DSP Toolkit will establish if the breach is reportable to the Information Commissioner Office (ICO) and full RCA is needed
If the breach is non-reportable, a full RCA is unlikely to be needed but the IG Team will liaise with the reporter to complete a short form RCA with recommendations. 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 ICB Route Cause Analysis (RCA)

Full 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. Guidance is attached in appendix 2.

1. CSU IG Team to discuss with the line-manager of the reporter, and the IG Lead for the ICB, 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 sent to the SIRO, DPO, CG, IG Lead, IG BPs and manager of the team
4. Manager of the team/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 report template.docx

Appendix B – RCA Guidance

Root Cause Analysis guidance.p