NHS
Shropshire, Telford
and Wrekin
Clinical Commissioning Group

NHS
Midlands and Lancashire
Commissioning Support Unit

Standard Operating Procedure

Information Governance Breach Reporting

Shropshire, Telford & Wrekin CCG

V1.0

Your NHS partner for **improving health** and **integrating care**

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 CCG Ref No.	Version 1.0 IG006
6	Publication Date	
7	Review Date	
8	Target Audience	All staff within Shropshire, Telford and Wrekin CCG
9	Cross Reference	Information Governance Data Security and Protection Policy and IG Handbook
10	Superseded Document	N/A
11	Approved by	Laura Clare (SIRO) and Alison Smith (CG)
12	Contact Details	MLCSU IG Team Email: mlcsu.ig@nhs.net Tel: 01782 872648

Version	
V1.0	New document for new single organisation

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 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):

DO NOT INCLUDE ANY PERSONAL IDENIFIABLE INFORMATION IN THE FORM	
What has happened? Include details as much as you can about what happened including:	
Job role of the person who has caused the breach, which team are they in and which organisation are they employed by?	
What information has been breached, i.e. name, address, full CHC record etc? This needs to be specific, including if any particularly sensitive data such as sexual health, mental health, safeguarding data etc.	
How did the breach occur?	
Where has the information gone?	
How was the information sent, i.e. post, email etc and please state if this was a secure encrypted method if known?	
Has it been accessed and seen by someone inappropriately?	
Has the information been returned, double deleted, or otherwise securely destroyed and not further saved used or shared? **If not, this should be done immediately, and actions confirmed by recipient.**	
If relevant, has the information now been sent to the correct recipient?	
If the information was pseudonymised (i.e. data subjects initials or NHS number, patient ID etc) could the recipient identify the individual, for example using a system they currently access? If they can identify the individual is that because they have a legal basis (within their job role) to have the information, but it was not sent using the correct process?	
How did you find out, how did you become aware?	
When did you become aware? date and time	
Was the incident caused by a problem with a network or an information error? (This could be a technical or system error).	
What is the local ID for the incident	To be determined by IG

Who is the data controller? (Note, it can only be the CSU IF the data subject is a CSU member of staff). Otherwise it must be a CCG. The data controller is the organisation who controls how the information of the data subject is processed. CHC always process patient data on behalf of a CCG, therefore that CCG would be the data controller.	
When did the incident start? (This is when the breach actually occurred?	
Is it still ongoing? (Is the information still at risk or has it been fully mitigated). Yes or no	
When did the incident end? **(When was the breach fully mitigated?)** Date the incident stopped	
Have the data subjects been informed? Yes/no/planned – to be decided by the Caldicott Guardian	
Does the incident impact across a national border? Yes or No	
If yes, have you notified overseas authorities? **Yes or No**	
Have you informed the Police? Yes or No	
Have you informed any other regulatory bodies about the incident? i.e. GMC, H&SE CQC. If yes, who and reference number If yes, who?	
Has there been any media coverage that you are aware of? Yes or No	
What other actions have already taken place or are planned? (What have you already done to mitigate the breach and what are you planning to do? This could include requesting the information is returned or securely destroyed).	

How many citizens affected? (How may data subjects’ information have been breached. This could include next of kin information on a letter regarding a patient).			
Who is affected, i.e. children, vulnerable adults, staff, patients, next of kin? (Please consider if the information breached contains any personal data about other data subjects, next of kin for example)			
When scoring the breach below, it is important to be conscious of the type of information that has been breached, who is affected and who has inappropriately accessed the information. Could this have an impact on the data subject and if so, how big an impact? How likely is it that the impact will actually occur?			
What is the likelihood that individuals’ rights have been affected?	**Not occurred**	**There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence**	Yes or No
	Not likely	**In cases where there is no evidence that can prove that no adverse effect has occurred.**	Yes or No
	Likely	**It is likely that there will be an occurrence of an adverse effect arising from the breach.**	Yes or No
	Highly likely	**There is almost certainty that at some point in the future an adverse effect will happen.**	Yes or No
	Occurred	**There is a reported occurrence of an adverse effect arising from the breach.**	Yes or No
What is the severity of the adverse effect, none, potential, some effect, pain, suffering, financial or death?	**No adverse effect**	**There is absolute certainty that no adverse effect can arise from the breach**	Yes or No
	Potentially some minor adverse effect or any breach involving vulnerable groups even if no adverse effect	**A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include**	Yes or No

	occurred	**possible inconvenience to those who need the data to do their job.**	
	Potentially Some adverse effect	**An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health**	Yes or No
	Serious - potentially Pain and suffering/ financial loss	**There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.**	Yes or No
	Death / catastrophic event	**A person dies or suffers a catastrophic occurrence**	Yes or No

These 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 CMS 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 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. The SIRO should notify the Board of all reportable breaches.

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 reporter, 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 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

2020-09-16 Breach
Reporting Form.docx

Appendix B – RCA Guidance

Root Cause
Analysis guidance.p

NHS RightCare
CYBER ESSENTIALS
CIMA Chartered Institute of Management Accountants PREMIER PARTNER
disability confident EMPLOYER
FUTURE FOCUSED FINANCE LEVEL 2 ACCREDITED
CIPFA CPD ACCREDITED EMPLOYER
aat accredited employer
CIPS PROCUREMENT EXCELLENCE
CIPS PROFESSIONAL ETHICS
GCHQ Certified Training
APMG International Accrediting Professionals
APPROVED ACCA EMPLOYER
APPROVED ACCA EMPLOYER
HSJ VALUE AWARDS 2019
HSJ VALUE AWARDS 2019
HIGHLY COMMENDED OF THE GO UK PUBLIC PROCUREMENT NATIONAL AWARDS
west midlands ACADEMIC HEALTH SCIENCE NETWORK
HSJ VALUE AWARDS
PENNA
PEN National Awards 2016
Re:thinking the experience

Standard Award
Number: 0503 – Valid to: 06/2022

0604
VALID TO 08/05/2020

For CyberStrong (our cyber security course)

Professional Development

Trainee Development - Gold

FINALIST
PHARMACY AND MEDICINES OPTIMISATION AWARD

FINALIST
CLINICAL SUPPORT SERVICES AWARD

30 April 2019
Hilton Metropole,
Birmingham
goawards.co.uk

Mental Health Innovation Award 2017
Innovative Organisation of the Year 2016

Winner: Value and improvement in use of IT to drive value in non-clinical support services 2016 (with Birmingham CrossCity CCG)

Winner: Commissioner of the Year 2016

Get to know us or get in touch

mlcsu

Midlands and Lancashire Commissioning Support Unit

midlandsandlancashirecsu.nhs.uk