NHS Corby Clinical Commissioning Group

NHS Nene Clinical Commissioning Group

Data Security and Protection Incidents Cyber Security Incidents and Near Misses Reporting Procedure

Procedure Number: **IG05**

Version:	3.0
Approved by:	Information Governance Working Group
Date approved	May 2018
Ratified by:	Audit and Risk Committee
Date ratified:	July 2018
Name of originator/author:	Louise Chatwyn – Information Manager
Name of responsible individual:	Neil Boughton – Deputy Director of Corporate Affairs
Review date:	May 2020
Target audience:	All Staff

Version Control Sheet

Version	Date	Who	Change
1.0		G Lawrence	
1.1	07/13	M Griffiths	Review for CCG ownership
1.2	09/13	M Griffiths	Changes made re feedback from Audit & Risk August 2013
2.0	04/16	L Chatwyn	Review and update to current
2.1	04/16	L Chatwyn	Incorporation of Audit feedback
2.2	05/16	L Chatwyn	Incorporation of Consultation minor amendment
2.3	07/17/	L Chatwyn	Minor revisions to reflect current legislation and practice and changes under the General Data Protection Regulations (GDPR)
3.0	05/18	L Chatwyn	Revisions to reflect new reporting Incorporate Corby CCG

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 came into UK Law on 25 May 2018. It introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Security of Network and Information Systems Directive ("NIS Directive") also requires reporting of relevant incidents to the Department of Health and Social Care as the competent authority from 10 May 2018

This document details what constitutes a Data Security and Protection Information Incident, Near Miss and Cyber Security Incident. It sets out Corby CCG and Nene CCGs procedures for the effective management of such incidents to ensure compliance with all appropriate legislation, and standards

NOTE: NHS Digital has released guidance for the Notification of Data Security and Protection Incidents which can be located within the front pages of the DSP Toolkit https://www.dsptoolkit.nhs.uk/Help/29 The guidance is referenced throughout this document

2. Purpose

All organisations processing health and adult social care personal data are required to use the Data Security and Protection Toolkit Incident Reporting Tool to record incidents.

The report level will determine the need for onward reporting to Department of Health (DH), Information Commissioner's Office (ICO) and other regulators.

NOTE: The European Union General Data Protection Regulation (GDPR) came into force in all EU Member States from 25 May 2018. GDPR replaced the Data Protection Act 1998 which is supplemented by the Data Protection Act 2018

Under the GDPR, breach notification is mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Certain breaches incur a reduced reporting time.

Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach[1].

This document is a statement of the approach and intentions for Corby and Nene CCGs to fulfil their statutory and organisational responsibilities. It will enable

[1] SOURCE: https://www.eugdpr.org/ Article 34

management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of the CCGs.

This document covers all aspects of information, in both paper and electronic format.

The CSU provide a managed security service to the CCGs for Information Management & Technology (IM&T). This includes support to the Senior Information Risk Officer on security and asset and risk management.

The CSU will manage security along current best practice guidelines as provided by DH and in accordance with applicable legislation. Information Security risks relating to Cyber Security will be referred to the CSU IM&T Team

Where information security incidents of fraud are identified, they may be referred to the Local Counter Fraud Specialist

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	The CCGs SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Corby CCG and Nene CCG is the Chief Finance Officer

Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Corby CCG is a Clinical Executive The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO for the CCGs is fulfilled by NEL CSU Email: nelcsu.dpo@nhs.net Phone: 03000 428438
Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardian of information risks and information incidents
Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for co-ordinating analysis, investigation and upward reporting of events and recommendations for remedial action to prevent recurrence and ensure compliance and continuing improvement
Managers	Managers and supervisors are responsible for • ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority. • ensuring the initial training compliance of all staff reporting to them
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual Data Security and Protection training • Report information Incidents appropriately

5. What is a breach?

A breach is defined as;

Article 4(13) “Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data is defined as;

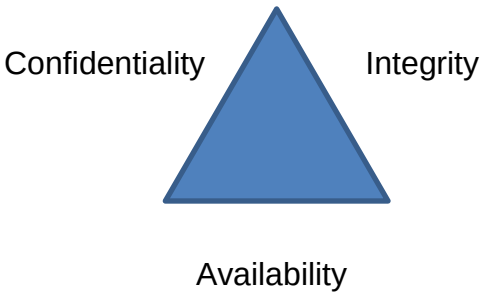
“any information relating to an identified or identifiable living individual”
And an “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to— (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

The GDPR definitions, notification and subject communication requirements will include breaches that organisations might not have notified under the previous data protection regime. The view that a data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a ‘risk to the rights and freedoms of individuals’ under Article 33 of GDPR.

Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner via the reporting tool.

6. Types of breach

The three types of breaches as defined in the Article 29 Working Party on Personal data breach notification are Confidentiality, Integrity or Availability (CIA)



- Confidentiality Breach – unauthorised or accidental disclosure of, or access to personal data
- Availability Breach – unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity Breach – unauthorised or accidental alteration of personal data

These are further outlined in the table below which incorporates the Article 29 Working Party categorisation of confidentiality, integrity and availability breaches compared to historic SIRI and Cyber SIRI classifications

Type of breach Art 29 WP	Sub type Art 29 WP	SIRI tool	Cyber SIRI tool	ICO categorisation including new cyber breach types
Confidentiality				
	Unauthorised or accidental disclosure	B Disclosed in Error	Phishing emails	Data sent by email to incorrect recipient
		H Uploaded to website in error	Social Media Platforms	Data posted or faxed to incorrect recipient
		J Unauthorised Access/Disclosure	Spoof website	Failure to redact data
			Cyber bullying	Information uploaded to webpage
				Verbal disclosure
				Failure to use bcc when sending email
				Data sent by email to incorrect recipient
				Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)
				Cyber incident (phishing)
	Unauthorised or accidental access	I Technical security failing (including hacking)	Hacking	Insecure webpage (including hacking)
		J Unauthorised Access/Disclosure		Cyber incident (key logging

				software)
Availability				
	Unauthorised or accidental loss	A) Corruption or inability to recover electronic data	Denial of Service (DOS)	Loss or theft of paperwork
		C Lost In Transit		Loss or theft of unencrypted device
		D Lost or stolen hardware		Loss/theft of only copy of encrypted data
		E Lost or stolen paperwork		Data left in insecure location
				Cyber incident (other – DDOS etc.)
				Cyber incident (exfiltration)
				Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)
	Unauthorised or accidental destruction	F Non-secure Disposal – hardware	Malicious internal damage	Insecure disposal of paperwork
		G Non-secure Disposal – paperwork		Insecure disposal of hardware
Integrity				
	Unauthorised or accidental alteration	K Other	Web site defacement	Other principle 7 failure
				Cyber incident – unknown (e.g. data published on Pastebin but no information on how compromise occurred)

7. When is an incident reportable under GDPR

Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner (SIRO) when determining what the significance and likelihood a data breach will be.

The significance is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5 1 being a non occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to a vulnerable group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

Grade the potential significance of the adverse effect on individuals

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	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.
4	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.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Establish the likelihood that adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Both the adverse effect and likelihood values form part of the breach assessment grid

There are a limited number of circumstances where even when an organisation is aware of a breach of personal data there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances notification may not be necessary;

- encryption – Where the personal data is protected by means of encryption.
- 'trusted' partner - where the personal data is recovered from a trusted partner organisation.
- cancel the effect of a breach - where the controller is able to null the effect of any personal data breach

Breach Assessment Grid

This operates on the 5x5 basis with anything other than “green breaches” being reportable. Incidents where the result is in the red grading are advised to make notification within 24 hours

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

Impact	Catastrophic	5	5	No impact has occurred	10	An impact is unlikely	15	20	25
							Reportable to the ICO DHSC Notified		
	Serious	4	4		8		12	16	20
	Adverse	3	3		6		9	12	15
							Reportable to the ICO		
	Minor	2	2		4		6	8	10
					No impact has occurred				
	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						

Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following it must still be reported as a level 2 and as such notifiable to the ICO.

If a breach involves certain categories of vulnerable groups it must be scored as a minimum 2 on both axes of the scoring matrix although it may be higher depending on the severity or likelihood but will not In all circumstances be notified to the ICO;

For clarity special categories under GDPR not listed below 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

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,
- and the processing of genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation

By criminal convictions and offences under Article 10 of the GDPR , this has the further meaning listed in the Data Protection Act 2018 Part 2, Chapter 2, S11 (2) and is taken to include –

(a) the alleged commission of offences by the data subject;

or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing

Assessing risk to the rights and freedoms of a data subject

The GDPR gives interpretation as to what might constitute a 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

8. What to include in the notification

Article 34 of the GDPR outlines what must be communicated to the relevant authority and this has been included in this reporting tool

The GDPR requires that the following information be included in any notification;

- A description or the nature of the personal data breach including, where possible, the categories and approximate number of data subjects

concerned and the categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer or other contact point from whom more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

9. Process – How to report an incident?

Initial information is often sparse and it may be uncertain whether a SIRI has actually taken place. Suspected incidents and 'near misses' should still be reported and can be recorded on the Data Security and Protection Toolkit Incident Reporting Tool, as lessons can often be learnt from them and they can be closed or withdrawn when the full facts are known

The reporting template can be found at Appendix 1

Where it is suspected that an IG SIRI has taken place, it is good practice to informally notify key staff (the Information Team, SIRO, Caldicott Guardian) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'.

For cyber incidents the Information team will liaise with the person(s) responsible for Information Technology (IT) and Information Security (IS)

Where fraud is identified it will be referred to the Local Counter Fraud Specialist

10. Reporting Timescales for Information Incidents

The 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. 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.

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. This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware.

Incidents where the result is in the red grading are advised to make notification within 24 hours

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.

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.

If requested by the regulator such as the Information Commissioner the local file of the investigation must be passed to them.

11. Communication of a personal data breach to the data subject

Under the GDPR, data processors will also be required to notify their customers, "without undue delay" after first becoming aware of a data breach

Article 34 of the GDPR states

1. '*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay'*
2. *'The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)'*

12. Monitoring and Review

Performance against key performance indicators will be reviewed on an annual basis through the Data Security and Protection Toolkit submission and used to inform the development of future documents.

Toolkit Data Security Standard 6

All staff are trained in how to report an incident. [The Board] understands that it is ultimately accountable for the impact of security incidents, and bear the responsibility for making staff aware of their responsibilities to report upwards

Unless there is major legislation or policy, this document will be reviewed annually

13. Training

Appropriate Data Security and Protection training will be provided to all staff annually.

Training is available through ESR which can be found here:
http://www.esrsupport.co.uk/access.php

14. Distribution and Implementation

All policy and procedural documents in respect of Information Governance will be made available via the intranet where this is in place

Staff will be made aware of procedural updates as they occur via team briefs, management communications, shared drive availability and notification via the CCG staff intranet where this is in place.

15. Associated Legislation and Documents

To include but not limited to:

- IG01a – Framework CSU Information Governance Framework
- IG01b – Policy CSU Information Governance Policy
- IG02a – CCG Physical Assets
- IG02b – Data Assets (application provider guide)
- IG03 – CCG Information Disclosure and Sharing Policy and Procedure
- IG04 – CCG Email and Internet
- IG06 – CSU Confidentiality & Data Protection Policy
- IG07 – CCG/CSU Data Protection Impact Assessment Procedure
- IG08a – Framework CSU Information Security Framework
- IG08b – CCG Information Security Policy
- IG09 – CCG Safe Haven Procedure
- IG10a – Framework CSU Information Quality Framework
- IG10b – CCG Records Management Policy
- IG11 – CCG Subject Access Request
- IG12 – CSU Freedom of Information Policy and Procedure
- Anti-Fraud and Bribery Policy

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Data Protection Act 2018
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- General Data Protection Regulation (GDPR)

16. References

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/

The EU General Data Protection Regulation
https://www.eugdpr.org/

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Data Security and Protection Incident Reporting tool
https://www.dsptoolkit.nhs.uk/News/31

The NHS Constitution for England
https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

NHS Code of Confidentiality
https://www.england.nhs.uk/wp-content/uploads/2013/06/conf-policy-1.pdf

NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

17. Appendices

Appendix 1 Reporting Form

A word copy of the reporting form is available from the Information Team

Information Security Incident Reporting Form

Email completed forms as soon as possible to nccg.informationgovernance@nhs.net
Provide as much information as you can, but do not delay sending in the form.
Please note that data breaches must be reported to the supervisory authority within 72 hours

GENERAL DETAILS	
Incident number:	*To be added by Information Governance*
Department/Section:	
Reporting officer:	
Investigated by:	
Contact number:	
Date form completed:	
Date and time of incident:	
Location of incident	

ABOUT THE INCIDENT	
Incident description. What has happened?	
How was the incident identified?	
What information does it relate to? eg. a file containing details of 100 service users name, address, direct debit details.	
What medium was the information held on? - Paper - USB stick - laptop, etc	
If electronic, was the data encrypted?	
Dealing with the current incident: **Please list initial actions:** **-** Who has been informed? - What has been done?	
Are further actions planned? If so, what?	
Have the staff involved in the security incident completed Data Security Awareness Training?	

If so, what and when? (Please list)	
Preventing a recurrence: Has any action been taken to prevent recurrence?	
Are further actions planned? If so, what?	

IMPACT ASSESSMENT QUESTIONS		
1.	**Was any data lost or compromised in the incident?** eg. loss of an encrypted laptop will not actually have compromised any information, unless eg. the user was logged in when they lost it.	Yes/No
2.	**Was personal data lost or compromised?** This is data about living individuals such as service users or employees. This could be a breach of the General Data Protection Regulations	Yes/No
3.	**If yes, was <u>sensitive</u> personal data compromised?** This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, potential or actual criminal offences, genetic or biometric. This could be a serious breach of the General Data Protection Regulations	Yes/No
4.	**Was adult social care, health or public health data involved?**	Yes/No
5.	**What is the number of people whose data was affected by the incident?**	
6.	**Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals? Physically, materially, or morally?** Example - physical harm, fraud, reputation, financial loss,	Yes/No
7.	**Did people affected by the incident give the information to the CCG in confidence?** (ie. with an expectation that it would be kept confidential)	Yes/ No
8.	**Is there a risk that the incident could lead to damage to individuals eg. via identity theft/ fraud?** eg. loss of bank details, NI numbers etc.	Yes/No
9.	**Could the incident damage an individual's reputation, or cause hurt, distress or humiliation eg. loss of medical records, disciplinary records etc.?**	Yes/No
10.	**Can the incident have a serious impact on the reputation of the CCG?**	Yes/No
11.	**Has any similar incident happened before in the section?**	Yes/No
12.	**Please confirm you have contacted HR for advice regarding this incident, if applicable**	Yes/No
13	**If this incident involves the loss or theft of IT Equipment please confirm you have logged a call to the IT Help Desk?**	Yes/No

FURTHER ACTION: (to be completed by Information Governance)	
Completed by:	
Is further action required?	Yes/No
Have data subjects been informed?	Yes/No
Have key stakeholders been informed?	Yes/No
Have control weaknesses been highlighted and recommendations made?	Yes/No
Has sufficient and appropriate action been taken?	Yes/No
Does the incident need reporting to Caldicott Guardian/SIRO?	
Does the incident need reporting to the ICO?	Yes/No
Does the incident need reporting on the IG toolkit	Yes/No
Does the incident need reporting to CSU Information Security Manager?	Yes/No
Has the Incident Log been updated?	Yes/No

Further investigation undertaken by:-	
Date incident closed:-	

You can also contact the following for advice:

Information Team and Corporate Services
X 1436/1202