Approved Sept 2020

North West London
Collaboration of
Clinical Commissioning Groups

Data Security & Protection Breaches
Information Governance Incident & Information Security & Cyber Incident Reporting

Policy and Procedure

Version 2.0

Version Control

Version Number	Reviewing Committee / Officer	Date
1.0	NHS NW London Clinical Commissioning Group, IT Security & Cyber Security Team	10/12/18
1.1	Abhilash Abraham	21/01/19
1.2	Reviewed by Local Counter Fraud Specialist team (RSM)	19/11/19
1.3	NWL DPO	24/06/20
2.0	RSM	21/09/20

Reviewers

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Abhilash Abraham		IT Security & Cyber Security Lead	7 Mar 2019	1.2
Dr. Ernest Norman-Williams		Head of Information Governance & Data Protection Officer	7 Mar 2019	1.2
Dr. Ernest Norman-Williams Felicia Ayo-Ajala		Data Protection Officer (GP) Data Protection Officer (Corporate)	24 June 2020 24 June 2020	1.3

Approvals

This document must be approved by the following:

Title	Signature	Title / Responsibility	Date	Version
Jenny Greenshields		CFO/SIRO	21 September 2020	2.0

Table of Contents

1. Introduction

NHS North West London Collaboration of Clinical Commissioning Groups (hereafter referred to as the NWL CCG) is committed to a programme of effective risk and incident management. The NWL CCG has a responsibility to ensure data breaches and / or information governance incidents are reported and managed efficiently and effectively.

The General Data Protection Regulation (GDPR) brought in in May 2018 requires that where personal data breaches affect the 'rights and freedoms of an individual,' Article 33 (of GDPR) imposes a duty to report these types of personal data breach to NHS Digital and to the Information Commissioner's Office (ICO). In some cases, these will also be reported to Department of Health and Social Care (DHSC). These are reported using the Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

This procedure explains the system to be used for staff for the recording, reporting and reviewing data security and protection breaches / incidents. This supports the NWL CCG's overall incident reporting process which is an integral part of personal, clinical and corporate governance.

The information contained within this procedure is taken from the "Guide to the Notification of Data Security and Protection Incidents" produced by NHS Digital (May 2018). Further detailed information about data breach reporting can be found in this document and must be referred to when reading this procedure and grading any personal data breach / incident. The guidance can be found on the following link:

https://www.dsptoolkit.nhs.uk/Help/29

It is a contractual requirement to include statistics on personal data breaches in the annual report and the Annual Governance Statement presented to the Board and the NWL CCG must keep a record of any personal data breaches, regardless of whether it is required to notify these to the ICO. The Information Governance (IG) Team co-ordinate and maintain a Data Security Breaches / Incident Reporting Logbook.

The NW LCCG is not subject to the Security of Network Information Systems (NIS) Regulations 2018 and is therefore not required to report breaches under this regulation.

2. Purpose

This document sets out the directions across the NWL CCG for the reporting and management of Data Security & Protection breaches / incidents. This includes: IT incidents/Breaches and Information Governance incidents/Breaches.

For those staff covered by a letter of authority / honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the NWL CCG.

Further, this procedure applies to all third parties and others authorised to undertake work / process data on behalf of the NWL CCG.

3. Definitions

Personal Data Breach

As per Article 4(12) of the GDPR, a "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.

The traditional view that a personal 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. These types of breaches are graded as per the guidance from NHS Digital using a risk scoring 5x5 matrix and maybe notifiable to the Information Commissioners Office (ICO) if they attain a grade as described in the guidance.

Personal data

This is data defined as any information relating to an identified or identifiable living individual.' An "Identifiable living individual" means a living individual who can be identified, directly or indirectly, 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.

All paper records that relate to a living individual and any aspect of digital processing such as IP address and cookies are deemed personal data. GDPR also introduces geographical data and biometric data to be classified as personal data.

Special Categories of Personal Data

Under GDPR, these are:

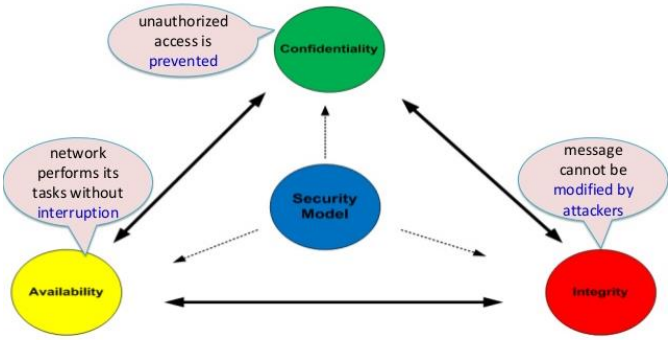
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data
- biometric data for uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

For data security breach reporting purposes, special categories of data also 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

Breach Types

The Article 29 working party, an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission now known as the European Data Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR) from 25th May 2018 categorised data security breaches into 3 categories which were associated with confidentiality, integrity and / or availability.



A definition of each category of breach is detailed below:

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

personal data
- Integrity Breach – Unauthorised or accidental alteration of personal data

Table 1 below states the ICO categorisation of data breaches in conjunction with the type of breach category as identified by the Article 29 Working Party.

Please note further details regarding the types of breaches under each of the CIA Triad can be found in the "Guide to the Notification of Data Security and Protection Incidents" guidance in Appendix 1.

Table 1 – ICO and Article 29 Working Group classification of data security breaches

	ICO Categorisation	Type of Breach (Art 29 Working Party)
A	Data sent by email to incorrect recipient	Confidentiality
B	Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)	Confidentiality
C	Cyber incident (phishing)	Confidentiality
D	Insecure webpage (including hacking)	Confidentiality

	ICO Categorisation	Type of Breach (Art 29 Working Party)
E	Cyber incident (key logging software)	Confidentiality
F	Loss or theft of paperwork	Availability
G	Loss or theft of unencrypted device	Availability
H	Loss/theft of only copy of encrypted data	Availability
I	Data left in insecure location	Availability
J	Cyber incident (other - DDOS etc.)	Availability
K	Cyber incident (exfiltration)	Availability
L	Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	Availability
M	Insecure disposal of paperwork	Availability
N	Insecure disposal of hardware	Availability
O	Other principle 7 failure	Integrity
P	Cyber incident - unknown	Integrity

4. Roles and responsibilities

Accountable Officer

Has ultimate responsibility for the implementation of the provisions of this policy and procedure. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support incident reporting for Data Security and Protection incidents. .

Data Protection Officer (DPO)

This role is required as per the General Data Protection Regulations (GDPR). The DPO's role is to inform and advise the NWL CCG and its staff about their obligations to comply with the GDPR and other current data protection laws. They are required to monitor compliance with the GDPR and current data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

For the purposes of incident reporting, the DPO will provide advice and guidance around the grading and categorisation of any Data Security and Protection Incident, and in the event of a reportable incident to the ICO, will be the point of contact.

Caldicott Guardian

To review and provide feedback regarding an incident where this relates to patient data. This may involve decision making about informing patients regarding an incident or not if this would deem to cause them harm / distress.

Senior Information Risk Owner (SIRO)

To review data security and protection incidents and report issues to the Audit Committee and Senior Management Team and ensure that any external reporting of the incident if required is undertaken

Information Governance and IT Security and Cyber Security Team have responsibility:

- To co-ordinate and investigate reported data and security protection incidents, maintain the NWL CCG Incident / Data and Security Breaches Reporting Logbook, make recommendations and act on lessons learnt.
- To liaise with the, NWL CCG IG Leads, NWL CCG SIRO and NWL CCG IT Manager as appropriate pertaining to data security incidents.
- To escalate incidents to the SIRO, DPO, Caldicott Guardian as appropriate.
- To grade the incident and report it where necessary on the Data and Security Breaches Reporting Toolkit Incident Reporting Tool and local NWL CCG IG

Incident / Data Breaches Logbook.

NWL CCG IT Operations Lead

- To work with the IT Security Manager to investigate the incidents where IT and IT Security input is required, make recommendations and act on lessons learnt.
- To liaise with IG Leads as appropriate especially regarding reporting.
- To inform the Senior Information Risk Owner, DPO, Caldicott Guardian as appropriate.

IT and Cyber Security Manager/Lead

To alert the NWL CCG IT Lead, IT Security Manager and nwlccgs.igenquiries@nhs.net when a member of NWL CCG staff reports a potential or actual information security incident / IT / cyber security incident that is reportable as per the NHS Digital process via the IT Service Desk. This can then be investigated, reported and graded accordingly on the Data Breaches / Incident Reporting Logbook and the DSPT Incident Reporting Tool if this requires escalation and reporting to the ICO / NHS Digital.

Line Managers

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to reporting data security & protection breaches / incidents.

NWL CCG Employees

Staff and members are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment term of office with the NWL CCG and this extends after they have left the NWL CCG.

5. Data Security Breaches / Incident Investigation Process

All data security breaches / incidents, whether it is an IT incident or an Information Governance incident must be reported to the NWL CCG IG Lead DPO **AS SOON AS THE INCIDENT IS KNOWN** following the NWL CCG's incident reporting processes (detailed below):

For IT incidents/breaches, staff must complete the NWL CCG IT Security Incident Reporting form (Appendix 3); this should be submitted to the IT security team generic email address: nwlccgs.security@nhs.net. A copy of the form can also be found on the intranet under Informatics/IT Security and Cyber security. For an IG data incident/breach, complete the IG Incident reporting form (Appendix 4) and risk assess the incident in conjunction with your line manager as appropriate. Fully

completed form should be submitted to nwlccgs.igenquiries@nhs.net. Also send a copy to the Information Governance Team / DPO.

Staff should not delay the reporting of any incident even if unsure whether it may not be a breach / incident. If it is identified as a data security breach / incident, it will be logged on the NWL CCG Data Security Beaches / Incident Reporting Logbook/Tool.
.

The NWL CCG will continue to utilise its own internal incident reporting procedure for the management of incidents. All incidents must be reported initially to the nwlccgs.igenquiries@nhs.net . The immediate response to an incident and the escalation process for investigation or external reporting will vary according to the severity level of the incident.

Where incidents are identified as a Data/Cybersecurity / IG incident the NWL CCG IG Lead will liaise with the DPO and the SIRO.

The IG Leads will log this on the local NWL CCG Data Security Breach / Incident Reporting Logbook/Tool.

Incident Grading

Incidents are graded according to the significance of the breach on a scale of 1-5 (1 being the lowest and 5 being the highest) and the likelihood of those serious consequences occurring on a scale of 1-5 (1 being the lowest and 5 being the highest). Please note incident / breaches are graded according to the impact on the individuals it concerns and not the organisation.

Article 34 requires the NWL CCG to notify the relevant authority when an incident constitutes a high risk to the rights and freedoms of an individual. This is classified when a breach 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

The tables in Appendix 1 set out how to grade the severity of a personal data breach / incident to see if it is high risk and be significant enough to be reported to the ICO. The Breach Assessment Grid in Appendix 2 ascertains when an incident is notifiable and to whom. The DPO is responsible for reporting any breach that is likely to result in high risk to

the rights and freedom of an indivudual to the ICO as appropriate.
When incidents are notifiable, this is carried out using the NHS Digital Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

Vulnerable Groups

Where a data security breach relates to a vulnerable group in society, a minimum risk assessment score of 2 for likelihood and significance is stated unless the incident has been contained.

Time scale for reporting

Article 33 of GDPR requires reporting of a breach within 72 hours of becoming aware of the breach to the ICO as appropriate. This is from when the NWLCCG becomes aware of the breach and may not be necessarily when it occurred. However, it is important that all staff report any IG incidents / breaches AS SOON AS POSSIBLE. Failure to notify promptly may result in action taken by the ICO by breaching Article 33.

It is mandatory for all staff to report 'near misses' as well as actual incidents, so that we can take the opportunity to identify and disseminate any 'lessons learnt'.

Informing the public

Article 34 requires that the public are notified if a data security breach results in a high risk to the rights and freedoms of individuals. In summary, this notification must include a description of the breach, name and contact details of the DPO or equivalent, a description of the likely consequences of the breach and a description of the measures taken or to be taken to address and mitigate the breach and its possible adverse effects.

If the NWL CCG decides not to notify individuals it must have a justified reason to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals it concerns.

Containment Actions which affect notification status

There may be circumstances where the NWL CCG is aware of a breach but there are containment actions that remove the need for notification to the ICO. This will still be recorded locally. For example, notification may not be necessary when:

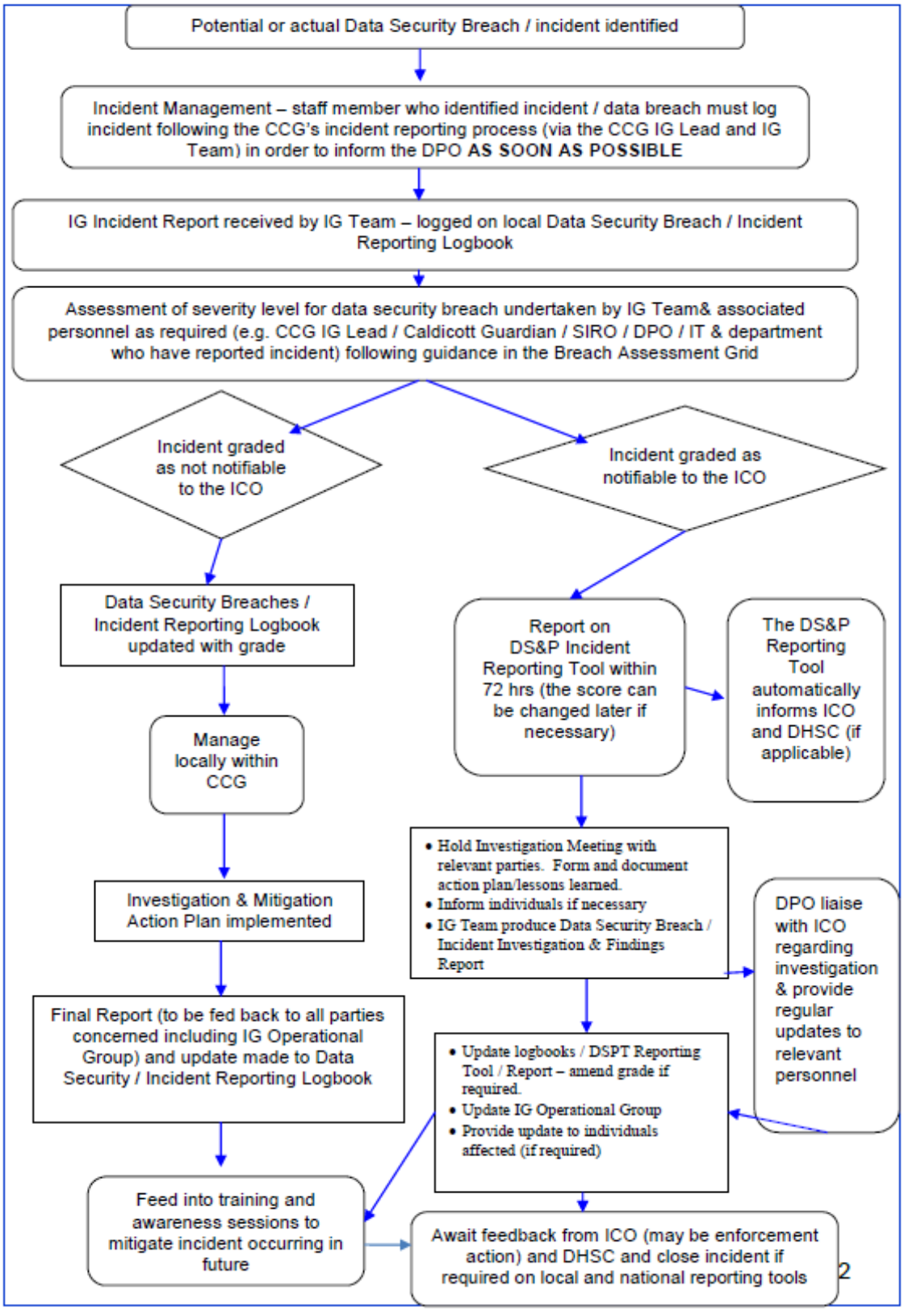
- Encryption is used to protect personal data
- Where personal data is recovered from a trusted partner organisation. A trusted partner is classified when the controller (NWL CCG) may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error and to comply with instructions to return it. Even if

the data has been accessed, the NWL CCG could still possibly trust the recipient not to take any further action and return and co-operate with the NWL CCG's instructions

- Where the NWL CCG can null the effect of any personal data breach

The flowchart (Figure 1) sets out the overall process for reporting, managing and investigating data security and protection incidents / personal data breaches for the NWL CCG.

Figure 1 – Data Security Breach / Incident Reporting Flowchart



6. Reporting

Reporting in the Annual Governance Statement / Statement of Internal Control

Reportable incidents that affect the rights and freedoms of an individual need to be detailed in the annual report / governance statement / Statement of Internal Control as outlined in Table 1 and Appendix 3 & 4 below.

Table 1 - Summary of Data Security and Projection Incidents reported to the ICO and/or Department of Health and Social Care (DHSC)

Date of incident (month)	Nature of incident	Number affected	How patients were informed	Lesson learned

Reporting by NHS Digital

Data breaches reported via the DSPT Incident Reporting Tool will be forwarded to the appropriate organisation indicated in the guidance such as the Department of Health and Social Care (DHSC), NHS England and the ICO. Additionally, these organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident information may be shared onward. For this reason, it is prohibited to include individual information that could identify any person affected by a breach. All incidents will be shared on a quarterly basis in aggregate form for incident monitoring and trend analysis.

Reporting to the LCFS

Where there are actual or attempted data breaches that may involve an element of fraud, these should be reported to your Local Counter Fraud Specialist for further investigation. The contact details for your LCFS – Erin Sims 07800 617456, erin.sims@nhs.net. Alternatively visit your intranet page for further details and information.

Reporting to the NWL CCG's Audit Committee

Data Security breaches / incidents are reported routinely at the NWL CCG's Information Governance Operational Group, which reports to the NWLCCG's Audit Committee. Lessons learned are discussed and actioned when necessary to assist mitigation of future similar incidents.

7. Closure and Lessons Learned

It is essential that action is taken to help to minimise the risk of data breaches / IG incidents re-occurring in the future. Therefore, all data breaches / IG incidents that are reported will be logged and any associated lessons learned will be fed back to staff. This may be communicated via email / staff briefings / team meetings.

Staff involved with a data breach / IG incident should consider with their line manager if additional training and support is needed. The investigation team and / or IG Team will determine this. Line managers should contact the IG Team for further assistance.

8. Training and Awareness

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the NWL CCG and this extends after they have left the employ of the NWL CCG.

Individual staff members are personally responsible for any decision to pass on information that they may make.

All staff are responsible for adhering to the Caldicott Principles, the Data Protection Act 2018, General Data Protection Regulation, the Confidentiality Code of Conduct, the National Data Guardian Security Standards and the common law duty of confidentiality.

Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy /strategy and procedure manuals; line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings); staff Intranet;

All staff are mandated to undertake Data Security training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Information Governance policy.

9. Monitoring and review

This procedure will be reviewed every two years, and in accordance with the following on an as and when required basis:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

10. Legislation and related documents

A set of procedural document manuals will be available via the NWL CCG's website.

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the NWL CCG staff Intranet.

A number of other policies are related to this policy and all employees should be aware of the full range below:

- ISMS
- https://nhsnwl.oak.com/Home/Index/5f846f8d-fea3-47cd-bc47-2f518ad57b35

Acts Covered Under Policy

- General Data Protection Regulation
- Data Protection Act 2018

Appendix 1 - Guide to Notification of Data Security & Protection Incidents

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.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity 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

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

Appendix 2 – Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable / notifiable to the ICO / DHSC via the DSPT incident reporting tool.

Incidents where the grading results are in the red are advised to be notified within 24 hours.

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				

Reportable to the ICO DHSC Notified

Reportable to the ICO

No Impact has occurred

An impact is unlikely

Appendix 3 – IT Incident Reporting Example Form

SECTION A: CONTACT INFORMATION		
REPORTED BY:	PRACTICE & CCG :	DATE REPORTED:
TITLE:	PRACTICE MANGER & TELEPHONE:	
LANDESK REF NO:	EMAIL:	
SECTION B: IDENTIFYING DETAILS WHEN APPLICABLE		
MAKE/MODEL	SERIAL NUMBER	Is this an SI : YES/NO
STATE TAG NUMBER:	COMPUTER NAME:	
WAS CONFIDENTIAL DATA INVOLVED, IF SO DESCRIBE:		
WAS DATA ENCRYPTED, DESCRIBE:		
ESTIMATED VALUE OF THE COMPUTING DEVICE:		
SECTION C: INCIDENT DETAILS		
DATE AND TIME OF INCIDENT:		
TYPE OF MEDIA: ☐ ELECTRONIC ☐ PAPER		
TYPE OF DEVICE: ☐ PC ☐ LAPTOP ☐ BLACKBERRY/PDA ☐ MOBILE PHONE ☐ OTHER (DVD/CD/UFD) If not above TYPE OF BREACH :		
WAS PATIENT IDENTIFIABLE DATA STORED/VIEWABLE IN THIS CASE/ : YES/NO – (Brief Details) . CLASSIFICATION OF DATA: ☒ CONFIDENTIAL ☐ SENSITIVE ☐ PERSONAL ☐ N/A (explain below)		

TYPE OF INCIDENT: ☐ **THEFT** ☐ **LOSS** ☐ **DAMAGE** ☐ **DESTRUCTION** ☐ **MISUSE** ☐ **UNAUTHORIZED MODIFICATION / RELEASE OF INFORMATION (complete Sections B, D, E)**
DESCRIPTION OF INCIDENT:
INDIVIDUALS INVOLVED/AFFECTED BY INCIDENT:
AREA(S) INVOLVED WITH INCIDENT:
WERE OTHER EMPLOYEES INVOLVED: ☐ **Yes** ☐ **No**
LOCATION/ADDRESS OF INCIDENT:
WAS INCIDENT REPORTED TO (IG, IT SECURITY ETC.) & DATE:
POLICE REPORT NUMBER (IF APPLICABLE):
HAVE THOSE RESPONSIBLE FOR THE INCIDENT BEEN IDENTIFIED?: ☐ **Yes** ☐ **No** ☐
IMPACT OF INCIDENT:

IG CONTACTED: ☐ **Yes** ☒ **No**	**INCIDENT #**	**OFFICER NAMES:**
ESTIMATED COST OF INCIDENT:		

SECTION D: CORRECTIVE ACTIONS (IT SECURITY OFFICER'S RECOMMENDATION
ACTIONS TAKEN TO PREVENT RECURRENCE:

ADDITIONAL RECOMMENDED ACTIONS:		
ESTIMATED COST OF CORRECTIVE ACTION: $		
SECTION E: REPORTING SOURCE/ISO SIGNATURE (IT SECURITY/PRIVACY OFFICER		
PREPARER NAME:	**TITLE:**	**TELEPHONE:**
ISO SIGNATURE :		**DATE REPORTED:**

Review of actions taken after incident

No.	Brief description of action	Date completed	Outcome of action	Further action required?
1	**e.g.** Reported to the police	**e.g.** 20 Aug 18	**e.g.** Police attended her home address. Statement given to police and crime reference number issued to her	**e.g.** Police to follow up and update her on case progress
2				
3				
4				
5				
6				
7				
8				
9				
10				

Appendix 4 –Information Governance Incident Reporting Form

Article 4(12)GDPR: The law defines a personal data breach as a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Incident Summary:

Process in place:

Action Points:

INFORMATION GOVERNANCE INCIDENT REPORTING FORM

Incident Details

Incident Date		**Incident Time**		**Date of incident report**	
Location of Incident					
			CCG/ Borough presence		
Independent Contractor			**Other**		
Incident location address:					

Description of Event *(Enter Facts not opinions, Do not enter names of people)***:**

.

Immediate Action Taken *(Enter action taken at the time of the event or immediately after)*:

Surname:		First Name:	

The following checklist helps evaluate the severity of this incident. Please check the appropriate boxes.

Type of Incident:

Staff inappropriately viewing records/documentation without a legitimate business related purpose.	
Insecure disposal of information	☐
Actual or attempted theft of information	☐
Loss of information within CSU premises *(including electronic media and paper based records)*	☐
Loss of information from outside CSU premises *(including, for example, theft from employee home or car)*	☐
Information lost in transit *(including, for example, post, courier, loss by a contractor or third party supplier)*	☐
Unauthorised disclosure of information.	☐
Fax/Email/letter sent in error to the wrong recipient	☐
Information sent by insecure means.	☐
PC terminal/laptop left unattended and logged in	☐
Discussing confidential matters in an open area where the conversation can be overheard.	☐
Personal information left unattended in a public space within the Organisation	☐

Scale of Incident:

1	Information about less than 100 individuals	☐
2	Information about 101 to 1000 individuals	☐

3	Information about 1001 to 100,000+ individuals	☐

Sensitivity Factors:

Low	
No clinical data at risk	☐
Limited demographic data at risk e.g. address not included, name not included	☐
Security controls/difficulty to access data partially mitigates risk	☐
Medium	
Basic demographic data at risk e.g. equivalent to telephone directory	☐
Limited clinical information at risk e.g. clinic attendance, ward handover sheet	☐
High	
Detailed clinical information at risk e.g. case notes	☐
Particularly sensitive information at risk e.g. HIV, STD, Mental Health, Children	☐
One or more previous incidents of a similar type in past 12 months	☐
Failure to securely encrypt mobile technology or other obvious security failing	☐
Celebrity involved or other newsworthy aspects or media interest	☐
A complaint has been made to the Information Commissioner	☐
Individuals affected are likely to suffer significant distress or embarrassment	☐
Individuals affected have been placed at risk of physical harm	☐
Individuals affected may suffer significant detriment e.g. financial loss	☐
Incident has incurred or risked incurring a clinical untoward incident	☐

Whether an IG Incident is to be externally reported depends on the context, scale (number of individuals affected), and sensitivity. If the investigation deems that there are minimal risks to the individuals affected, the incident will be reported and logged internally for monitoring and accountability purposes along with a justification as to why the incident was deemed as low risk. This log will be disclosable to the ICO and auditors auditing the CCG's breach reporting procedures. Where investigations deem that the incident is likely to result in a risk to the rights and freedoms of natural persons, it will be reported to the ICO by the Data Protection Officer and the DH by the Information Governance Manager via the IG Incident Reporting Tool. In the case of a reportable personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

Notification:

Has a decision been taken to notify the individuals affected	

Details of the incident reporter:

Name	
Date	
Email Address	
Telephone	
Your Line Manager	

What happens next?

Please pass the form to your line manager for review, risk assessment and investigation. Forms should then be submitted to **nwlccgs.igenquiries@nhs.net**. Please, also send a copy to the Information Governance Team / DPO. Thank you for completing the incident form.

Please risk assess this incident

Name		**Job Title**		**Date**	

Risk Assessment:

	Likelihood of incident happening at that severity				
Severity of incident	**1**	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 No harm	1	2	3	4	5

Please assess the risk grade of the incident prior to investigation using the Matrix above (Likelihood x Severity=) and record:

The risk grading will help identify the level of investigation required.

Investigation Details:

Please provide details about the investigation that has been undertaken following the incident:

.

Please list any contributory factors and root causes that you have identified through your investigation of the incident. **Continue on a separate sheet if necessary.**

1.	
2.	
3	

Actions:

Please list any actions which have been or will be taken to reduce the impact of this incident or the risk of it happening again. **Continue on a separate sheet if necessary.**

	Action Required	Person Responsible	Due Date
1.			
2.			
3.			

Re-Assess the Risk:

Following investigation you should re-assess the risk posed in light of the actions planned to mitigate the risk. Use the matrix at the top of this page (Likelihood x Severity=) and record the grade here:

Once completed:

Email the form to: nwlccgs.igenquiries@nhs.net

Thank you for taking the time to report this incident.

Appendix 5: Key Contacts

NWLCCG Information Governance Team:

ICT Security & Cyber Security Lead
Abhilash Abraham
Email: abhilash.abraham@nhs.net

Data Protection Officer (GP)
Ernest Norman-Williams
Email: ernest.norman-williams@nhs.net

Data Protection Officer (Corporate)

Felicia Ayo-Ajala

Email: Felicia.ayo-ajala1@nhs.net

Senior Information Risk Owner (SIRO)
Jenny Greenshields
Email: jenny.greenshields1@nhs.net

NWLCCG Caldicott Guardian
Diane Jones
Email: diane.jones11@nhs.net@nhs.net

Appendix 6

Policy for the development, ratification and implementation of and related Procedural documents

Equality Impact Assessment Tool (Equality Analysis)

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/ No	Comments
1	**Does the policy/guidance disadvantage one group or more than another on the basis of:**		
	• Race (including colour, culture, ethnicity, nationality or national origin and the travelling community)	N	
	• Religion or Belief	N	
	• Sex (e.g. male or female)	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual)	N	
	• Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.')	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (children, young adolescent, older people etc.)	N	
2	**Is the policy/guidance/strategy more favourably towards one group on the basis of:**		

	• Race	N	
	• Religion or Belief	N	
	• Sex	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation	N	
	• Gender reassignment	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (e.g. children, young adolescent, older people etc.)	N	
3	**If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.**	N/A	
4	**Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?**	N/A	
5	**If so, how would you address the impact? Please explain.**	N/A	
6	**What are the associated objectives to the policy/guidance?**		See section 2 of policy

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.