IG Breach Reporting Policy

1. INTRODUCTION

This Policy is one of a suite of policies and procedures relating to the management of information for chevin

The procedures apply to incidents that impact on the security and confidentiality of personal information. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

These information incidents can be categorised by their effect on patients and their information:

- Confidentiality e.g. unauthorised access, data loss or theft causing an actual or potential breach of confidentiality;
- Integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information;
- Availability, e.g. records are missing, mis-filed, or have been stolen, compromising or delaying patient care

These procedures apply to all staff including permanent, temporary, and locum

1. Managing Incidents

The Practice has assigned the role of incident manager to the Practice Manager, who in conjunction with the Data Protection Officer (art 37 GDPR) will assess and manage all GDPR/IG and Data Protection Breaches. The practice DPO is Paul Couldrey and can be contacted as below: -

PCIG Consulting Limited
Mobile: 07525 623939
E-mail: Couldrey@me.com

Any actual or potential information incident in the Practice will be assigned to one of the following categories (the list is not exhaustive) and investigated and managed accordingly.

GDPR reporting Requirements

The GDPR will introduce a duty on all Practices to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected (art 33).

The practice only must notify the relevant supervisory authority of a breach where it is likely to result in a **risk to the rights and freedoms of individual**s. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The above must be assessed on a case by case basis by the practice DPO and IG Lead. Therefore, a breach MUST be reported to the DPO and IG lead within 24 hours of the practice becoming aware of it so that an appropriate assessment can take place.

A) Breach of patient confidentiality

The Practice will;

- Interview the complainant to establish the reason for the complaint and why the Practice is being considered responsible;
- Investigate according to the information given by the complainant;
- Record findings, e.g. unsubstantiated concern, suspected/potential breach, actual breach, etc.;
- Where necessary, provide written explanation to the patient with formal apology if warranted;
- Take and document appropriate action, e.g. no further action as there is no evidence that information was put at risk, advice/training, disciplinary measures, etc.
- Report the breach to its commissioner and the supervisory authority (the Office of the Information Commissioner) via their DPO if appropriate within 72 hours of being aware of the breach.

B) Incorrect disposal of confidential material

This type of incident may lead to a breach of confidentiality and is likely to be reported by a patient affected, a member of the public, or a member of staff and could be paper, hard drive, disks/tapes, etc. ***The Practice will;***

- Investigate how the information left the Practice by interviewing staff and contractors as appropriate;
- Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g. breach of confidentiality, misuse of data;
- Consider whether the patient(s) should be informed and where it is judged necessary, provide written explanation to the patient(s) with formal apology;
- Record findings, e.g. potential breach, actual breach, evidence of misuse, etc;
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, etc.
- Report the breach to its commissioner and the supervisory authority (the Office of the Information Commissioner) via their DPO if appropriate within 72 hours of being aware of the breach

C) Attempted or actual theft of equipment and/or access by an unauthorised person

This type of incident may lead to a breach of confidentiality, the risk that information has been tampered with, or information not being available when needed. ***The Practice will;***

- Check the asset register to find out whether equipment is missing;
- Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base);
- If the cause is external inform the police, ask them to investigate and keep them updated with your findings;
- Interview staff and check the asset register to establish what data was being held and how sensitive it is;
- Establish the reason for the theft/unauthorised access, such as:
  - Items to sell;
  - Access to material to embarrass the Practice;
  - Access to material to threaten patients (blackmail, stigmatization).
- Consider whether there is a future threat to system security;
- Inform insurers;
- Review the physical security of the Practice;

- If there has been unauthorised access to the Practice computer system:
  - Ask the system supplier to conduct an audit to determine whether unauthorised changes have been made to patient records;
  - Consider whether any care has been provided to patients whose records have been tampered with;
  - Check compliance with access control procedures, e.g. ensure passwords haven't been written down, staff members are properly logging out, etc.
- Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate (e.g. warning patients);
- If computer hardware or the core software has been stolen, inform system suppliers to enable restoration of system data to new equipment;
- Record findings, e.g. potential breach, actual breach, evidence of tampering, compromised or delayed patient care, etc;
- Take and document appropriate action, e.g. physical security improvements, advice/training, disciplinary measures, etc.
- Report the breach to its commissioner and the supervisory authority (the Office of the Information Commissioner) via their DPO if appropriate within 72 hours of being aware of the breach

D) Computer misuse by an authorised user

This includes browsing medical records when there is no requirement to do so; accessing unauthorised Internet sites; excessive/unauthorised personal use, tampering with files, etc. ***The Practice will;***

- Interview the person reporting the incident to establish the cause for concern;
- Establish the facts by:
  - Asking the system supplier to conduct an audit on activities by the user concerned;
  - Interviewing the user concerned
- Establish whether there is a justified reason for the alleged computer misuse;
- Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g. breach of confidentiality; the risk information may have been tampered with; and consider whether the patient(s) should be informed;
- Record findings, e.g. breach of confidentiality, evidence of tampering, fraud, carrying on a business, accessing pornography, etc;
- Take and document appropriate action, e.g. no action as allegation unfounded, training/advice, disciplinary measures, etc.
- Report the breach to its commissioner and the supervisory authority (the Office of the Information Commissioner) via their DPO if appropriate within 72 hours of being aware of the breach

E) Lost or mis-filed paper medical records

This type of incident could have a possibly severe impact on patient care as the information within a patient record is incorrect or is not available when required. ***The Practice will;***

- Investigate who last used/had the paper record by interviewing staff and contractors as appropriate;
- Consider whether any care has been provided based on incorrect information within a patient record;
- Consider whether patient care has been delayed due to information not being available;
- Establish whether missing information can be reconstituted, e.g. from electronic records;
- If information within records has been mis-filed, ensure it is restored to correct filing order/returned to the correct record;
- Where necessary, (i.e. if care affected) provide a written explanation to the patient with formal apology;
- Record findings, e.g. compromised or delayed patient care, etc;
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, etc.
- Report the breach to its commissioner and the supervisory authority (the Office of the Information Commissioner) via their DPO if appropriate within 72 hours of being aware of the breach

2. Reporting incidents to external Practices

Article 33 of the GDPR requires that a notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the Practice becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

Serious information incidents, i.e. those categorised as level 2 - 5 in the table below are reported to NHS England, the Clinical Commissioning Group and the Information Commissioner. The practice IG lead and DPO will notify the appropriate authorities.

For GP's breaches should be reported via the Local CCG Patient Safety Email inbox as below:-

The e-mail address is {insert local CCG reporting mail}

Reporting categories for information incidents					
0	**1**	**2**	**3**	**4**	**5**
Minor breach of confidentiality affecting one patient	Potentially serious breach. Less than 5 patients affected or risk assessed as low, e.g. files were encrypted	Serious potential breach and risk assessed high, e.g. unencrypted records of up to 20 patients	Serious breach of confidentiality, e.g. up to 100 patients affected	Serious breach with either particular sensitivity, e.g. sexual health details, or up to 1000 patients affected	Serious breach with the potential for ID theft of over 1000 patients affected
Minimal discernible effect on the Practice - media interest unlikely	Damage to staff member's reputation. Possible media interest, e.g. celebrity involved	Damage to the Practice's reputation, some local media interest that may not go public	Damage to the Practice's reputation, low-key local media coverage	Damage to the Practice's reputation, local media coverage	Damage to the NHS' reputation, national media coverage

3. Lessons learned

All registered incidents are re-evaluated after a 6-month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those types of incidents has reduced. If there is no change in the volume of each type of incident the Practice Partner(s) are alerted and appropriate action taken

To provide staff with an example of what could occur, how to respond to such events and how to avoid them, previous incidents are used in security and confidentiality training sessions.

4. When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant Authorities as above, the practice should also consider Duties of Candour, the IHG Lead with the DPO will made the assessment about information individuals of any breaches.

5. Reporting Incidents

Incidents should be reported using the form below:-

GENERAL INFORMATION	
REGISTER NUMBER -	
Reported by:	Date/time discovered:
INCIDENT DETAILS	
Type of incident ***[tick a category]***: • **Confidentiality e.g. breach due to unauthorised access, potential breach due to lost record, etc;** • **Integrity, e.g. records altered without authorisation, etc;** • **Availability, e.g. records missing, mis-filed, theft etc.**	
Incident details, state the facts only, where it occurred; what information was involved; etc:	
Initial action(s) taken, what did you do, who will/have you reported to**:** **Date reported**:	
Investigation and management	
[Insert name and post of person investigating the incident] e.g. Information Governance Lead	**Date of commencement of investigation**
Investigations, findings, actions and recommendations:	
Post-incident reporting	
Incident and investigation outcome reported to [add any other relevant notes here, e.g. issue and outcome discussed at staff meeting]:	**Commissioning Practice YES/NO** **Information Commissioner YES/NO** **Practice Insurer YES/NO** **Other (e.g. Patient, Police)** [Insert details]

This initial reporting Form Must be sent to the practice DPO/IG Lead and Senior Partner within 24 hours of the incident being identified.

6. Approval

These procedures have been approved by the undersigned, and they will be reviewed on an annual basis and in particular in the event of an incident as part of the lessons learned process.

7. Training

Chevin must ensure that all staff undertake appropriate records management training on information governance issues soon after joining the practice and that existing staff receive periodic update training. Staff who have responsibility for records management should undertake records management training on an annual basis.

8. Equality and Diversity

The Practice aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Practice must have due regard to the Public-Sector Equality Duty (PSED). This applies to all the activities for which the Practice is responsible, including policy development, review and implementation.

9. Due Regard

This policy has been reviewed in relation to having due regard to the Public-Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

10. Review and Monitoring

The Practice Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.

This policy will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.