St Alban's Medical Centre

Data Breach Policy and Data Breach Register

Policy Statement

1. St Alban's Medical Centre (hereinafter referred to as the "the Practice") are committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

2. Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

Purpose

3. The purpose of this policy is to provide the Practice's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

Scope

4. This policy applies to all staff within the Practice (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Practice in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Data Security & Breach Requirements

5. The Practice's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6. We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject.

Objectives

7. Our objective are: -
   - To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
   - To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
   - To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches

- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees; including their information and identity
- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of any data breach (where applicable) with immediate effect and at the latest, within 72 hours of the Practice having become aware of the breach

Data Breach Procedures & Guidelines

8. The Practice has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

Breach Monitoring & Reporting

9. The Practice Manager is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

10. All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used.

Breach Incident Procedures

11. As soon as a data breach has been identified, it is reported to the direct line manager and the reporting officer immediately so that breach procedures can be initiated and followed without delay.

12. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Practice and is not about apportioning blame. These procedures are for the protection of the Practice, its patients, staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

13. As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

Breach Recording

14. The Practice utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome.

15. In cases of data breaches, the Practice Manager is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making

any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

16. A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

17. If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements, The Supervisory Authority protocols are to be followed and their 'Security Breach Notification Form' should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

18. Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

19. A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

20. Resultant employee outcomes of such an investigation can include, but are not limited to: -

    a. Re-training in specific/all compliance areas
    b. Re-assessment of compliance knowledge and understanding
    c. Suspension from compliance related tasks
    d. Formal warning (in-line with the Practice's disciplinary procedures)

System Error

21. Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with Healthcare Computing and any other linked system provider to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

22. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

    a. Attempting to recover any lost equipment or personal information
    b. Shutting down an IT system
    c. Removing an employee from their tasks
    d. The use of back-ups to restore lost, damaged or stolen information
    e. Making the building secure
    f. If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

Assessment of Risk and Investigation

23. The Practice Manager should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches. The investigator should look at: -

- The type of information involved
- Its sensitivity or personal content
- What protections are in place (e.g. encryption)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

24. The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions**.**

Breach Notifications

25. The Practice recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Practice's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

Supervisory Authority Notification

26. The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

27. Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after the Practice becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

28. If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

29. The notification to the Supervisory Authority will contain: -

    - A description of the nature of the personal data breach
    - The categories and approximate number of data subjects affected
    - The categories and approximate number of personal data records concerned
    - The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
    - A description of the likely consequences of the personal data breach
    - A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

30. Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

31. Where the Practice acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

Data Subject Notification

32. When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

33. The notification to the Data Subject shall include: -

    - The nature of the personal data breach
    - The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
    - A description of the likely consequences of the personal data breach
    - A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

34. We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

35. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Record Keeping

36. All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Senior Partner and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Responsibilities

37. The Practice will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.