EXE EAR CARE

07533 126317
info@exeearcare.com
exeearcare.com

POLICY TITLE – Management of Personnel Sensitive Data
POLICY NUMBER – 009

Date authored – 23/09/2024 Next review – 22/09/2025

REFERENCE

A. Data Protection Act 2018
B. The Caldicott principles
C. Information Commissioners Office, Subject Access Requests (SAR)
D. NHS, Records Management Code of Practice

PURPOSE

1. Exe Ear Care is committed to protecting the privacy and security of personal data in compliance with the General Data Protection Regulation (GDPR), Caldicott principles, and all applicable data protection laws, ensuring the confidentiality of patient and personnel data. This policy outlines how we collect, store, manage, and disclose sensitive personal data, and how we respond to Subject Access Requests (SAR).

SCOPE

2. This policy applies to all employees, contractors, volunteers, and third parties working for or on behalf of Exe Ear Care. It covers all processing activities involving the personal data of:

    a. Patients and service users
    b. Employees and contractors
    c. Any other identifiable individual associated with the company

DEFINITIONS

3. GDPR (General Data Protection Regulation): EU regulation that sets guidelines for the collection and processing of personal information.

4. Caldicott Principles: Guidelines ensuring that patient information is shared securely and only when necessary.

5. SAR (Subject Access Request): A request made by an individual to access their personal data held by the company.

6. Personal Data: Any information relating to an identified or identifiable natural person.

7. Sensitive Data: Special category data, including health records, biometric data, and data revealing racial or ethnic origin, political opinions, or sexual orientation.

8. Data Controller: Exe Ear Care, who determines the purposes and means of processing personal data.

9. Data Processor: A third party that processes personal data on behalf of the Data Controller.

DATA PROTECTION PRINCIPLES

10. In line with GDPR, Exe Ear Care adheres to the following data protection principles:

    a. Lawfulness, Fairness, and Transparency: Data is processed lawfully, fairly, and in a transparent manner.
    b. Purpose Limitation: Data is collected for specified, legitimate purposes and not further processed in a manner that is incompatible with those purposes.
    c. Data Minimization: Only the minimum amount of personal data necessary for the purpose is collected.
    d. Accuracy: Personal data must be accurate and, where necessary, kept up to date.
    e. Storage Limitation: Data is stored for no longer than necessary.
    f. Integrity and Confidentiality: Data is processed in a manner that ensures its security, including protection against unauthorized access.

RESPONSIBILITIES

11. Data Protection Officer (DPO): The DPO is responsible for monitoring compliance with GDPR and other data protection laws, as well as the management of SARs.

12. All Employees and Contractors: Must follow the procedures in this policy and report any potential data breaches to the DPO immediately.

13. Senior Management: Oversee the implementation and enforcement of this policy.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

14. Exe Ear Care processes personal data under the following lawful bases:

    a. Consent: Obtained from patients for treatment and care.
    b. Contract: Processing is necessary for the performance of employment contracts.
    c. Legal Obligation: Compliance with legal obligations, such as health and safety laws.
    d. Vital Interests: Processing necessary to protect someone's life.
    e. Public Task: Processing for tasks carried out in the public interest, such as healthcare services.
    f. Legitimate Interests: Processing for the legitimate business interests of Exe Ear Care, provided it does not override individual rights.

DATA SECURITY AND CONFIDENTIALITY

15. All personal data must be stored securely on encrypted systems and accessed only by authorized personnel.

16. Printed materials containing sensitive data should be stored in locked cabinets when not in use.

17. Digital communications must be encrypted, and secure email systems should be used when transmitting personal data.

18. Staff must attend regular training on data security and GDPR compliance.

CALDICOTT PRINCIPLES

19. Exe Ear Care adheres to the following Caldicott Principles to protect patient confidentiality:

    a. Justify the purpose of every use of confidential information.
    b. Do not use confidential data unless it is absolutely necessary.
    c. Use the minimum necessary patient-identifiable information.
    d. Access to confidential information should be on a strict need-to-know basis.
    e. Everyone with access to personal data must understand their responsibilities.
    f. Comply with the law.
    g. The duty to share information can be as important as the duty to protect patient confidentiality.
    h. Ensure there is no personal data breach when sharing or transferring information.

SUBJECT ACCESS REQUESTS (SARs)

20. Individuals have the right to request access to their personal data under the GDPR.

21. SARs must be submitted in writing, and Exe Ear Care will verify the identity of the requester before disclosing any information.

22. The company will respond to SARs within one calendar month of receiving the request.

23. If the request is complex or involves large volumes of data, this period may be extended by a further two months. The individual will be informed of the reason for the delay.

24. No fee will be charged unless the request is excessive or repetitive, in which case a reasonable fee may be charged.

DATA BREACH RESPONSE

25. In the event of a data breach:

    a. The CEO must be notified immediately.
    b. An internal investigation will be conducted to assess the scope of the breach.
    c. If necessary, affected individuals and the Information Commissioner's Office (ICO) will be notified within 72 hours of the breach being identified.
    d. Remedial actions will be taken to prevent future breaches.

DATA RETENTION

26. Personnel data will be retained for the duration of employment and for a period of 6 years post-termination, in accordance with legal and regulatory requirements.

27. Patient records will be retained for at least 20 years post-treatment, in line with national healthcare regulations (Long term illness, or illness that may reoccur: Patient records, NHS, Records Management Code of Practice).

DATA SUBJECT RIGHTS

28. Individuals have the following rights regarding their personal data:

    a. Right to Access: Obtain a copy of their data and details of how it is processed.
    b. Right to Rectification: Request correction of inaccurate or incomplete data.
    c. Right to Erasure: Request deletion of personal data where there is no legitimate reason for its retention.
    d. Right to Restrict Processing: Request a temporary halt to processing.
    e. Right to Data Portability: Request that their data be transferred to another organization in a machine-readable format.
    f. Right to Object: Object to the processing of their data in certain circumstances.

THIRD-PARTY PROCESSING

29. Where Exe Ear Care uses third-party processors, such as payroll services or IT providers, written agreements will ensure compliance with GDPR, including:

    a. Ensuring that processors act only under our instructions.
    b. Ensuring that adequate security measures are in place to protect personal data.

AUTHORITY

30. This policy was written today the *23rd September 2024* and is enacted with immediate effect. All directors and employees of Exe Ear Care are to follow the guidance and direction within.

R. J. Toon
CEO.