AAYAN MEDICAL IMAGING LTD.

Data Protection and Security Policy

About this Policy:

At Aayan Medical Imaging Ltd., registered in England and Wales, No. 06547415. And registered office, Suite 125 Kingspark Business Park Centre, 152 – 178 Kingston Road, New Malden, KT3 3ST, England, we are committed to handling Personal Data with the utmost care and responsibility. As part of our operations, we may collect information about our current, past, and prospective suppliers, customers, contractors, and other users of our services. This data, whether stored on paper or digitally, is protected under legal frameworks such as the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and other related regulations.

This policy, along with referenced documents, outlines how we will process Personal Data that we collect from Data Subjects or receive from other sources. Our Data Users are expected to adhere to this policy when processing Personal Data on behalf of Aayan Medical Ltd. We take any breaches of this policy seriously, as they may lead to disciplinary action.

Our focus as a Data Controller carries specific responsibilities, and we acknowledge the potential for different obligations when acting as a Data Processor. We will review this policy at least annually and update it as necessary to ensure compliance with evolving legislation and best practices. The latest version will always be available on our website at AMI Ltd or through our Data Protection Officer. Thank you for your commitment to maintaining the integrity and security of Personal Data.

1.Purpose

This policy establishes a robust framework for managing and safeguarding personal data and confidential information handled by AMI Ltd, ensuring compliance with the UK Data Protection Act 2018 and the General Data Protection Regulation (GDPR). AMI Ltd recognizes the importance of protecting the privacy and security of personal data, emphasizing its commitment to maintaining confidentiality, integrity, and availability of data. This policy outlines the principles, responsibilities, and practices necessary to mitigate risks and protect against data breaches, unauthorized access, and misuse of information.

2. Scope

This policy applies to all individuals who process data on behalf of AMI Ltd, including employees, contractors, consultants, and any other authorized personnel. It covers all data and information in both electronic and physical formats, across all systems, devices, and facilities owned, leased, or used by AMI Ltd. The policy encompasses personal data of patients, employees, and other stakeholders, as well as any business-related data that may contain sensitive or confidential information, regardless of how it is stored or accessed.

3. Data Protection Principles

AMI Ltd adheres to the following data protection principles, as outlined in GDPR, to ensure that all personal data is handled in a secure, lawful, and ethical manner:

- Lawfulness, Fairness, and Transparency: AMI Ltd processes data lawfully, fairly, and in a transparent manner. Individuals are informed about how their data is used, who has access to it, and the purpose behind its collection.

- Purpose Limitation: Data is collected and processed only for specified, legitimate purposes, and is not used for other unrelated purposes without consent or legal basis.

- Data Minimization: AMI Ltd ensures that only data necessary for intended purposes is collected, minimizing data to what is strictly relevant.

- Accuracy: Personal data is kept accurate and up to date. AMI Ltd takes reasonable steps to correct or delete inaccurate information upon detection or notification.

- Storage Limitation: Personal data is retained only as long as necessary for its intended purpose. Regular reviews ensure that outdated data is securely deleted or anonymized.

- Integrity and Confidentiality: Data is protected from unauthorized access, processing, or loss, with technical and organizational security measures in place to ensure confidentiality and integrity.

4. Data Collection and Processing

AMI Ltd collects and processes personal data strictly as necessary to support business operations and provide quality services. This data processing is limited to:

- Provision of Medical Imaging Services: Personal and health-related data is collected to deliver accurate medical imaging services and provide quality care.

- Legal and Regulatory Compliance: AMI Ltd ensures data handling complies with legal obligations, including health and safety laws, employment regulations, and financial reporting requirements.

- Efficient Internal Administration: Personal data is processed to support administrative functions such as payroll, resource allocation, and employee management, ensuring operational efficiency.

5. Roles and Responsibilities

- Data Protection Officer (DPO): The DPO oversees data protection compliance, providing guidance on GDPR obligations and data privacy issues. They also monitor data handling, conduct audits, train staff, and liaise with the Information Commissioner's Office (ICO) in cases of serious data breaches.

- Employees and Contractors: Each employee and contractor is responsible for understanding and following data protection policies and practices, including the secure handling of data, minimizing risks of unauthorized access, and promptly reporting any suspected breaches to the DPO.

6. Data Security Measures

AMI Ltd employs technical and organizational measures to ensure data security. These measures include but are not limited to:

- Access Control: Strict access controls ensure only authorized personnel have access to data based on job role and necessity, minimizing exposure to sensitive information.

- Encryption: Sensitive data, especially personal and health information, is encrypted both at rest and during transmission to protect against unauthorized interception or access.

- Secure Storage and Disposal: Physical files are stored in locked areas, and electronic files are maintained on secure servers with redundancy. Obsolete data is securely disposed of.

- Network Security: AMI Ltd maintains a secure network infrastructure, including firewalls, anti-virus solutions, and intrusion detection systems, to protect against external threats.

- Device Management: Only authorized devices may access the network, with guidelines requiring password protection, screen-locking, and regular updates to mitigate potential risks.

7. Data Retention

AMI Ltd retains personal data only for as long as necessary to fulfill the purpose for which it was collected, considering legal and regulatory requirements. The DPO oversees data retention schedules and conducts regular audits to ensure compliance. Data that is no longer necessary is securely deleted or anonymized, minimizing risks associated with storing outdated information.

8. Data Subject Rights

AMI Ltd respects the rights of individuals regarding their personal data and ensures that these rights are upheld. These rights include:

- Right of Access: Individuals can request access to their personal data held by AMI Ltd, receiving a clear explanation of its processing.

- Right to Rectification: Individuals may request corrections for any inaccuracies or incomplete data.

- Right to Erasure: Individuals can request deletion of their data when it is no longer needed, processed unlawfully, or upon withdrawal of consent (if applicable).

- Right to Restriction of Processing: Individuals may limit data processing if they dispute its accuracy or legality, or if it's needed for legal claims.

- Right to Data Portability: Individuals may request a structured copy of their data to transfer to another service, where feasible.

Requests are handled promptly and in compliance with GDPR, with processes in place to verify identity and assess each request's legitimacy.

9. Breach Management and Incident Response

AMI Ltd is committed to detecting, containing, and mitigating data breaches. Any suspected or confirmed breach is reported immediately to the DPO, initiating a structured response process. This includes:

- Containment and Assessment: Immediate steps are taken to contain the breach and assess the scope of compromised data.

- Investigation and Documentation: A detailed investigation identifies the breach's cause and impact, with findings documented for review.

- Notification: Affected individuals and relevant authorities, including the ICO, are notified within statutory timelines if required by law.

- Review and Improvement: Post-incident analysis and review help strengthen security practices to prevent future occurrences.

10. Training and Awareness

AMI Ltd mandates regular data protection and security training for all employees and contractors to foster a culture of compliance. Training covers GDPR basics, data handling best practices, breach reporting procedures, and specific role-based instructions where applicable. Refresher training is conducted periodically to ensure awareness of evolving risks and regulations.

11. Monitoring and Auditing

Data protection practices are subject to regular audits conducted by the DPO. These audits evaluate data handling practices, assess security measures, and identify areas for improvement. Results are reported to senior management, and corrective actions are taken promptly to address any compliance gaps.

12. Policy Review

This policy is reviewed annually or in response to significant operational or regulatory changes. The DPO is responsible for ensuring that the policy reflects current data protection standards and legal requirements. Regular reviews help AMI Ltd remain compliant and address any new risks or procedural adjustments.

Document Control:

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of the AMI Ltd Information Security Management System, and the relevance of this document
- A change in the manner in which AMI Ltd manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident, formal review or an audit finding.

The current version of this Policy shall be recorded below.

REVISION HISTORY			
	DATE	**VERSION**	**DESCRIPTION**
	10-May-18	01	Initial revision for AMI Ltd
	06-May-19	02	Yearly Review and agreed by management

REVIEWED AND APPROVED FOR USE BY			
APPROVED BY	**DATE**	**VERSION**	**SIGNATURE**
Seear Z Khan Senior Management	10-May-18	01	Approved
Seear Z Khan Senior Management	06-May-19	02	Approved By Email

DOCUMENT DISTRIBUTION	
NAME	**RESPONSIBILITY**
All Employees, including Contractors and Temporary Staff	DPO