ISMS Policy

Policy Overview

The organization is committed to safeguarding the information and data of both the company and its clients from internal and external threats by implementing a robust framework with comprehensive controls, tools, and processes.

Objectives:

- **Ensure Confidentiality, Integrity, and Availability:**
- Protect the confidentiality, integrity, and availability of information and data at all times, including the availability of electronic protected health information (ePHI)
- **Manage Security Risks:** Identify and manage risks associated with information security, cybersecurity, and physical security effectively.
- **Promote Compliance:** Enforce compliance with information security and data privacy controls across all systems and Computer security helps to make the HIPAA Privacy Regulation work
- **Adhere to Requirements:** Comply with all relevant legal, regulatory, and contractual obligations of stakeholders and for computers and networks that store or transmit personal health information
- **Prevent Security Breaches:** Prevent data breaches from both internal and external sources.
- **Enhance Staff Competency:** Provide sufficient security training and support to all staff, ensuring they are competent in their roles through education, training, and experience. Communicate the significance of adhering to the Information Security Management System (ISMS) and meeting security requirements.

Implementation and Communication:

This policy will be communicated to all employees and any organizations working on behalf of the company. All employees and affiliated organizations are expected to support the implementation of this policy and ensure that their activities are conducted without posing risks to themselves, others, or the environment.

Review and Accessibility:

Top management will review this policy annually and make amendments as necessary. Archived versions of previous policies will be maintained. This policy will be made available to relevant stakeholders upon reasonable request. Protect the organizational and clients' information and data from internal and external threats by implementing framework with adequate controls, tools and processes.

Damodar Rao Gummadapu
Chairman

*Interested parties include customers, shareholders, employees, government agencies, regulatory bodies, emergency services (police, ambulance, firefighters, etc.), employees' families, media, suppliers, contractors, outsourced partners, publishers, service providers, etc.