

**Velan HIPAA Policy Statement:**

It is our policy to properly determine appropriate uses of personal Health information in accordance with the US governmental rules, laws, and regulations especially Health Insurance Portability and Accountability Act, Privacy rule. We have deployed Compliance program plan and enforced meticulously and audited for its effectiveness.

**Use and Disclosure of Protected Health Information:**

We are always committed to ensure privacy, confidentiality, and security of patients' health information as an essential business function in our processes and to sustain our business relationship with our clients.

The identified or classified Protected Health Information shall be accessed by the designated staff to the quantum on "Need to know" basis.

**Our Compliance Program Plan includes the following Safeguards for PHI Confidentiality, Integrity & Availability:****a. Administrative Safeguard:**

1. Definite documented organizational security policies and procedures
2. Designated security Officer (HIPAA Compliance Officer)
3. Background check for employee before induction
4. Confidentiality and Non Disclosure agreement for employees
5. Employee Training on information/data handling
6. Scheduled training
7. Role based File Routing/access control

**b. Physical Safeguard:**

1. 24 Hr's Manned Security Desk
2. Control of peripherals (Disabled duplicating facilities like USB Ports/Pen drives, CD & printers)
3. Declaration of media & devices during entry and exit
4. Secure Workstation
5. Inspection & Audit control
6. Backup, Media & Device Control Policy
7. CCTV Systems (Video Surveillance Systems)

**c. Technical Safeguard:**

1. Access Control (Role based File Access/Access Control Policy)
2. Antivirus with latest virus definition – Centralized Anti-Virus Server for effective monitoring and control (Antivirus Policy)
3. Hardware Firewall Box with automatic update of Antivirus, Intrusion, Anti-Spam Definition (Firewall policy)
4. Secured file transmission using Secure Shell (Private Tunnel Transmission) and encrypted data transmission
5. Data Destruction after data retention period
6. Change control & revision control
7. Terminal/Workstation Access control using enforced password & automatic log off
8. Periodic Enforced Password Change and auditing.
9. Audit/Access Trail maintenance

**Training and Awareness**

Every individual who access the classified PHI shall be inducted to awareness training during the employee induction process and before authorizing them to access the PHI.

Continual Refreshment training/program is conducted to make them up to date on the compliance plan and also to rectify any apprehension/clarifications they might have.

**Material Change**

Any material change in the Statutory Laws or practices shall be acquired through continual learning process and periodic information exchange through Internal Emails/Intranet and meetings.

**Continual Audit**

As an embedded system with our established Quality Management System the Access Trail of PHI is audited for any breaches or violations periodically. The reports are submitted for Management Review Meeting for further decisions/action plan.

**Mitigation**

For any breach or non compliance or of any unauthorized use or disclosure of protected health information is mitigated to the extent possible.

**Data Retention, Storage & destruction**

The data stored under central repository shall be given access through enforced login by providing exclusive authentication method for each authorized individual. The information stored in the central repository shall be accessed only by the System Administrator and the information is encrypted using minimum 128 bit encryption technology.

The classified data are destroyed in presence of HIPAA Compliance Officer after the defined data retention period and duly audited for its retrievable status. The data destruction report is submitted to the Management in a periodical manner.

**Sanctions**

Any individual found to be violating the organizational security/usage of PHI shall be subjected to thorough examination along with the records and access logs maintained. If any objective evidence found, appropriate disciplinary action including termination of the employment shall be made. The clients or the owners of the PHI shall be duly informed on the nature of breach and action taken as a part of Mitigation process.

- **End of the Statement** -

---