It shall be the policy of Seyyone to protect and safeguard "protected health information" (PHI) created, acquired and maintained on or behalf of Seyyone operations. We are committed to practices and procedures that are consistent with the standards mandated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which will assist our clients in complying with the regulatory requirements imposed upon them by HIPAA.

Seyyone considers the privacy, confidentiality, and security of patients' health information as an essential component of our business relationship with our clients. Safe and secure handling of the patient information provided to us by clients is a crucial aspect of our business, and we undertake this responsibility at all levels.

Recognizing that we may qualify as a "business associate" under the HIPAA standards with respect to the privacy of individually identifiable health information, Seyyone has revised its standard confidentiality agreement, and has formulated safeguards to ensure HIPAA Compliance

A designated full-time HIPAA Compliance Officer ensures effective compliance

Safeguards

It is the policy of Seyyone that appropriate physical safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards will include physical protection of premises and technical protection of PHI maintained electronically and administrative protection. These safeguards will extend to the oral communication of PHI. These safeguards will extend to PHI that is removed from this organization.

HIPAA Administrative Safeguards

Seyyone has implemented the following administrative procedures at their facilities to guard data integrity, confidentiality, and availability:

1. Has implemented procedures for restricting use and disclosure of Protected Health Information (PHI) to the minimum amount necessary.
2. All personnel are bound by PHI confidentiality and non-disclosure agreements
3. The antecedents of the employees are ensured through background checks
4. Termination Procedure is in place to prevent continued access to PHI by a terminated employee.
5. Periodic information and security training are conducted mandatory
6. Assigned security responsibility through designated HIPAA Compliance Officer

HIPAA Physical Safeguards

Seyyone has implemented the following physical safeguards to guard data integrity, confidentiality, and availability:

1. Seyyone has effective measures for its physical security, like round the clock manned security desk and digital smart card authenticated entry
2. Duplicating facilities are disabled to ensure that no PHI is taken out of office
3. Seyyone employees are trained on policies regarding use and disclosure of PHI.
4. Seyyone maintains a highly redundant environment. Failure of servers will not take the systems offline. Our redundancy measures include a power generator, solar panel and two internet providers.
5. Seyyone has been equipped with highly modernized fire detection and suppression system to avoid any fire hazards.

HIPAA Technical Safeguards

Seyyone provides technical safeguards to guard the data integrity, confidentiality, and availability in our services:

A. Access controls:
Each user is allowed to view/access only specific informations according to defined access rights.

1. Access is granted to personnel based on their roles and need for PHI
2. Automatic log off and Enforced Passwords security are deployed to ensure workstation security.
3. Passwords are changed at all levels as per the Password policy to ensure more control

B. Audit Controls

All activities at Seyyone are monitored and activity logs are raised and audited for security breaches

C. Transmission Security
1. Transmission security is achieved through 128-bit data encryption.
2. Internet Security is ensured through firewall

Training and Awareness

It is the policy of Seyyone that all members of our workforce have been trained on the policies and procedures governing protected health information and how Seyyone complies with the HIPAA Privacy and Security Rule. It is also the policy of Seyyone that new members of our workforce receive training on these matters within a reasonable time after they have inducted. It is the policy of Seyyone to provide training should any policy or procedure related to the HIPAA Privacy and Security Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of Seyyone that training will be documented and records maintained for the prescribed period.

Sanctions

It is the policy of Seyyone that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies.

Retention of Records

At Seyyone the HIPAA Privacy Rule records retention requirement will be strictly adhered to. All records designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. After the records retention time it will be destroyed as per the data destruction policy.

Mitigation

It is the policy of Seyyone that the effects of any unauthorized use or disclosure of protected health information be mitigated to the extent possible.