HIPAA POLICY

At the Service Provider, we are committed to maintaining the confidentiality of information entrusted to us by our clients, Business Associates / Subcontractors, especially individually identifiable personal information such as names, addresses, and Protected Health Information (PHI).

The Service Provider enables our customers to communicate with their employees, patients, vendors, and other health care providers, via email and text message while complying with HIPAA.

The Service Provider protects the confidentiality of information it receives by adhering to the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule governs the acquisition, storage, transfer and retention of Protected Health Information, in both electronic and paper formats. The Security Rule covers all information acquired, maintained or transferred electronically.

The Service Provider complies with all business associate obligations under HIPAA/HITECH, enabling us to provide the highest level of service to our health care provider customers.

The Service Provider follows the policies and practices it has documented in its HIPAA Policy and Procedure Manual. These documents cover areas such as:

- Physical security of electronic equipment used to acquire and store PHI
- Technical safeguards to prevent unauthorized access to PHI
- Training and awareness for staff members who have access to PHI

The Service Provider respects the privacy of personal health information and takes securing all PHI data seriously. The Service Provider’s services are HIPAA ready and enable practices using the system to comply with its obligations as a Covered Entity.

Use and Disclosures of Health Information:

The Service Provider assures the appropriate use and disclosure of PHI is done in the normal course of business and appropriate based on the contracts with clients. The Service Provider will assure appropriate and adequate safeguards are established to protect customers’ patient information from unauthorized use and disclosures; where use is defined as the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information; and where disclosure is defined as release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Breach Notification:

Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology Economic and Clinical Health Act

(HITECH), Modifications to the HIPAA Privacy, Security Enforcement and Breach Notification Rules under the HITECH Act (Omnibus Rule).

HIPAA Privacy Practices Policy & Procedures:

The Service Provider acknowledges the need for practices with accounting of disclosure, electronic access to PHI, fundraising and PHI, sale of PHI, research and PHI, and marketing and PHI. Through the normal course of business, the Service Provider does not take part in any activities that would fall under the classifications of: Fundraising Activities; Sale of PHI; Marketing and Research of PHI.

Risk Analysis and Management:

The Service Provider is focused on protecting the confidentiality, integrity, and accessibility of the PHI. The Service Provider will regularly and timely review threats and vulnerabilities to their organization and systems focused on protecting the confidentiality, integrity, and accessibility of PHI. The Service Provider will take the proper steps to mitigate and reduce the risks to the organization and the PHI maintained.

Workforce & Information System Security:

The Service Provider is committed to proper protection of all uses and disclosures of PHI that it stores and maintains on behalf of a covered entity, and accordingly it is committed to hold all workforce members responsible for the proper protection of privacy and security requirements. The Service Provider will assure that the workforce members logging into the electronic systems that contain PHI are only looking at information needed to complete the daily operational work. The Service Provider doesn’t have access to the information of each of the individual organizations that are in the system software. The Service Provider is focused on protection of the physical components of the business that store and maintain PHI for the organization. The Service Provider assures that limitations are put on the ability to provide physical limitations to any PHI. The Service Provider only allows the appropriate access to systems based on business need and client responsibility.

Security Incident & Contingency Plan:

To protect all electronic media used for patient care, the Service Provider will properly report and respond to all potential security incidents that occur within the organization. The contingency plan for The Service Provider system will focus on data backup, disaster recovery, emergency mode operation plan, testing and revision, and application and data criticality analysis. The Service Provider will assure adequate controls are in place through regular review and evaluation to protect the confidentiality, integrity, and availability of electronic PHI.

Business Associate:

The Service Provider will maintain a process to assure the information shared and used by subcontractors is properly protected and safeguarded as required in the HIPAA regulation. The Service Provider will enter into a written business associate agreement with all subcontractors that create, receive, maintain, or transmit PHI to support the business operations of the Service Provider. Associates/Subcontractors will be obligated to effectively maintain the privacy and security of PHI as required by HIPAA and the Service Provider.

Security Rule:

The Service Provider is required by the HIPAA Security Rule to assure that the integrity to the data that it stores and maintains has not been altered or destroyed in an authorized manner. The Service Provider will protect all ePHI that it stores, maintains, and transmits from improper alteration and destruction by implementing a combination of policy and technical solutions, in the maintenance, retention, and eventual destruction/disposal of PHI.

HIPAA Security Officer:

The Service Provider will assure that an individual is appointed to be the organization's HIPAA Security officer. The security officer is responsible for the oversight and management of the organization's compliance with the HIPAA regulations. The security officer is the individual who is responsible for assuring the development, awareness, and enforcement of all the HIPAA policy and procedures established meet requirements.

Timely Updates:

The Service Provider will assure timely and appropriate policies and procedures in order to comply with the HIPAA Privacy and Security Regulations; accordingly, documentation will be updated, maintained, stored in accordance with the regulations. If you have any questions or concerns regarding this notice, please contact: The Service Provider using the information provided on the The Service Provider's website.

Last updated: May 2020