***Training***

Periodic and ongoing compliance training is required for all employees. The training related to handling ePHI (Electronic Protected Health Information) and PII (Personally Identifiable Information) includes sessions on HIPAA Privacy and Security, HIPAA Updates and HITECH, and Data Security Overview.

**Policies – Employees**

Employees have a responsibility to:

* Comply with the HIPAA Compliance Program, PHI, PII as well as report any violations of these to the project compliance coordinator immediately
* Comply with all data protection policies
* Encrypt any mobile device that contains confidential data
* Ensure that all PHI sent over the Internet is always encrypted before it is sent
* Destroy any PHI or PII that you have (electronic or hard copy) from any previous clients unless you need the PHI or PII to continue to perform work for that client
* Avoid storing any PHI on your laptop, mobile phone, or other portable equipment whenever possible – for current or previous clients
* Never use another person’s logon name or credentials to access systems at any time
* Lock your laptop when leaving it unattended
* Shred documents when no longer needed – shredders or bins are required at client sites
* Employees must report lost or stolen technology immediately to the appropriate company’s personnel. If the equipment was stolen, the employee must also notify the appropriate police agency and provide a copy of the police report to the company.

**PHI or PII Breach Determination and Notification**

* Project team members who discover, believe, or suspect that PHI has been accessed, used or disclosed in a way that violates the HIPAA Privacy Rules; must immediately report such information to the appropriate personnel (legal or Compliance) who will determine what reporting requirements are applicable.

**Requests for Client PHI**

* Client PHI should only be requested if necessary for the assigned task. When requesting or sending PHI to a client you need to verify in written or verbal communications the expected protocol for the handling of the client PHI prior to transmission, including protocols for the request, transmission, handling, storage, and disposal of the PHI.
* The information that you should request should be for the minimum amount of data required and that the data be de-identified data by the client whenever possible. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

**Unsolicited Receipt of PHI**

* If you have received inappropriate or misdirected PHI please follow these steps as required; Reply to the sender of the material that a PHI request was not made; delete or properly dispose of the PHI and notify the appropriate personnel (legal or Compliance) that this event has occurred. Do not open or retain the unsolicited PHI.

**Approved Transfer Methods for ePHI**

The following are deemed as acceptable methods for PHI transfer. Before transmitting any PHI you need to verify both the sending and receiving parties and the expected data. If there is any discrepancy in the receipt of the data the data should be treated as an unsolicited receipt of PHI.

• **SFTP***:* The Secure File transfer application allows for high speed transfer for larger data set.

• **Encrypted Email**: Email system needs to have encryption protocols enabled for a high level of secured transmission with the clients, with additional security features to make it less vulnerable.