HIITES HEALTH INFORMATION PRIVACY POLICY

We at HIITES understand that the information we collect and process is personal. Keeping the health information confidential and secure is one of our most important responsibilities. We need this information to provide quality management services and to comply with certain legal requirements, we are committed to protecting the health information we collect and to follow all state and federal laws regarding protection of the information.

1. As applies to healthcare providers; we as a practice management company are also required to:
- make sure that information we collected is kept private
- tell you about our legal duties and privacy practices with respect to information we collect

2. This policy describes the practices of HIITES and that of:
- Any other company directly operated by HIITES
- Any third party we subcontracted to provide services to any of our clients
- All employees, staff, and other personnel of HIITES

3. How we may use information we collect and process:

The information, which includes any information collected from a client, may be used for the different purposes for example administrative, operational, and to evaluate the quality of the services etc. HIITES provide a wide range and variety of practice management services to healthcare providers in USA. For this reason, not all types of uses of information can possibly be described in this document. We have listed some common examples of permitted uses and disclosures below.

For Treatment: Caregivers, such as nurses, doctors, therapists and social workers, may use the information we collect to provide healthcare services.

For Billing: HIITES may release information collected to health plan or health insurance carrier to obtain payment for the services provided by its clients. For example, we may need to give health plan information about a clinical exam or medications.

For Operations: HIITES may use to ensure that the services provided to its clients are high quality.
To Keep You Informed: Unless you provide us with alternative instructions, we may contact you about reminders for treatment, medical care, payment delays etc.

Following are the set of rules we follow at HIITES to ensure protection of all patient information.

1. Information Privacy Training

Staff undergoes structured information privacy training prior to delivering services remotely to any healthcare provider in any healthcare facility. During the training courses following materials are focused on:
   1. History and purpose of *Information Privacy Training*
   2. What type of information is protected and in what formats?
   3. The "minimum necessary rule" and the definition of a breach
   4. Best practices: examples of appropriate use and misuse of personal health information
   5. Consequences for violating information privacy
   6. How to report violations

2. Security of and Access to Electronic PHI

At HIITES, following measures are undertaken to ensure protection of electronic health information:

- Staff's access to EMRs is compliant with health information privacy security requirements.
- Each individual staff is issued a unique login or user identification with a secure password in order to gain access to any electronic system housing electronic health information.
- Generic staff logins or shared logins are not permissible, as unique identifiers are required in order to track each user's activity and system access in accordance with the HIPAA Security Rule.
- During any type of training, both a "trainer" staff and a "trainee" have their own individual logins or user identification.
- Staffs are forbidden to share login information or passwords and are required to regularly change their passwords.

3. Application of privacy regulations to the online environment

As our lives become increasingly electronic with the growth in use of such social media outlets as staff are educated that the principles taught during privacy training also apply to the online and social media world.