CHIS, Inc. and HIPAA

CHIS, Inc. provides services to healthcare facilities and uses certain protected health information (PHI) in connection with performing these services. Therefore, CHIS, Inc. is classified as a Business Associate, as defined by the regulations described in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. CHIS, Inc. complies with all state and federal guidelines regarding protection of patient health information, adhering to HIPAA guidelines that pertain to Business Associates. PHI is managed in electronic (ePHI) and paper-based format, and is used as necessary and required for performance of contracted duties. Occasionally, PHI is transmitted verbally over the telephone.

With the introduction of the HITECH act of 2009, HIPAA privacy and security compliancy for Covered Entities are also required by their Business Associates. CHIS, Inc. has always been at the forefront of compliancy and as such has had policies and procedures in place for HIPAA privacy and security. Along with continuing evaluation of current policies and procedures, CHIS, Inc. has designated a Security Officer for such purposes.

CHIS, Inc. Privacy General Guidelines

CHIS, Inc. acknowledges its obligation as a Business Associate for maintaining the security and confidentiality of PHI. In addition, CHIS, Inc. complies with HIPAA requirements for the management of PHI, in accordance with the following guidelines:

- **CHIS, Inc. will ensure the confidentiality, integrity, and availability of all PHI that is created, received, maintained or transmitted.**
- **CHIS, Inc. will protect against any reasonably anticipated threats or hazards to the security or integrity of such information.**
- **CHIS, Inc. will protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the Privacy subpart.**
- **CHIS, Inc. will ensure compliance with the Security subpart by our workforce.**

CHIS, Inc. Workforce Education and Training

- **CHIS, Inc. is proactive in providing appropriate security awareness training for all members of the workforce (including management) prior to assignment of duties that involves access to and use of PHI.**
- **CHIS, Inc. emails out a weekly HIPAA briefing on privacy and security news to all its' workforce for continuing training and reminders of the importance of privacy and security.**

Security

The HIPAA Security Rule adopts standards for the security of ePHI to be implemented by Covered Entities. The Health Information Technology for Economic and Clinical Health Act, or the HITECH Act, which was signed into law on February 17, 2009 as part of the economic stimulus package, required Covered Entities' Business Associates to comply with the Security Rule. Business Associates are contractors who create, maintain or have access to a Covered Entity's protected health information. CHIS, Inc. falls under the envelope of a Business Associate and use the HIPAA Security Rule standards to develop and maintain the security of all electronic individually identifiable health information on systems under it's control.

The Security Rule consists of security standards that CHIS, Inc. addresses to safeguard the central principles of security.

- **Confidentiality** - preventing unauthorized disclosure of sensitive information.
- **Integrity** - preventing unauthorized modification of systems and information.
- **Availability** - preventing disruption of service and productivity.

Access Control

CHIS, Inc. Access Control policy addresses ePHI access to be managed in a manner that is in compliance with all state and federal guidelines regarding protection of patient health information, including all HIPAA guidelines that pertain to Business Associates.

- **Unique User Identification**
- **Emergency Access**
- **Automated Log Off**
- **Data Encryption**

Emergency Access

- **CHIS, Inc. has a business continuity policy in place to ensure the processes of the workflow remain constant in the event of an emergency. Such instances include but are not limited to fire, vandalism, terrorism, system failure, or natural disaster.**
- **CHIS, Inc. follows a server back up policy. Stored ePHI is backed up on password protected security encrypted backup tapes stored inside a fireproof safe locked with a key.**
- **An audit log of responses to emergencies is kept.**

Automated Log Off

- **All office workstations are to be logged off after every workday. Users are to log off their systems after their workday and screen savers are used to password lock the display after 15 minutes of idle time.**
- **The Technology and Support Assistant will make sure all workstations have been logged off at the end of every workday. A log will be kept to record and notify users of when they fail to log off their workstations at the end of their day.**
- **Domain policy enforces an automatic log off from all workstations from designated users in our office environment.**

Data Encryption

- **Data in motion is any data that is in transport across public networks. All data transported from CHIS, Inc. network over public network infrastructures are secured using VPN and/or SSL encryption technology.**
- **Data at rest is any data that is stored on network hard drives and other devices. All data stored on CHIS, Inc. network servers are password protected and encrypted. All server data is backed up onto encrypted password protected backup tapes every night. All portable and stationary workstations do not have ePHI stored.**

Data Integrity

CHIS, Inc. ensures that data integrity of PHI is dependable and accurate, and in a manner that is in compliance with all state and federal guidelines regarding protection of patient health information, including all HIPAA guidelines that pertain to Business Associates.

- **Data Integrity**
- **Data Accuracy**

Data Integrity

Server Backups

CHIS, Inc. implements a server backup procedure which backup all saved ePHI to a separate media which is then stored in a key locked fireproof safe. The key to the safe is locked in a protected box.

Restore Testing

CHIS, Inc. implements a backup audit restore test every three months. The restore test results are logged and any issues with the restore are to be investigated and resolved. The Technology and Support Assistant will follow the procedure for incident tracking if required.

Data Accuracy

All of the PHI CHIS, Inc. accesses are located primarily on client networks connected to over secure VPN/SSL connections. Accuracy audits are performed on those systems by their administrators. We ensure data accuracy by ensuring that only the people who need access to those systems, have it and follow policies on data and electronic resource acceptable use policy and audit user access to client systems.

Backup Restore procedures are audited for accuracy to the original files.

Entity Authentication

CHIS, Inc. ensures that persons and entities are authenticated to ePHI and are verified and audited in a manner that is in compliance with all state and federal guidelines regarding protection of patient health information, including all HIPAA guidelines that pertain to Business Associates.

- **Entity Authentication**
- **Entity Verification**

Entity Authentication

Domain Authentication

CHIS, Inc. network resources use a domain controlled environment where user access and authentication is performed by the network server domain controller. Username and passwords follow the policy and access controls. Passwords change according to the policy and users will be the only one to know their unique passwords for authentication.

Remote Authentication

CHIS, Inc. has remote coding staff that connect to our network via an IPSec VPN connection. The VPN client is configured for three way handshake with AES 256 bit encryption with username and password authentication. Passwords and key exchanges are encrypted and secured. Username and passwords are granted by CHIS, Inc. IS for VPN authentication.

Clients

CHIS, Inc. connects to client networks to access PHI and is supplied the necessary credentials to log into their systems. Clients control their own username password policies and follow authentication processes that CHIS, Inc. are subject to. Connections to client systems are always using secured SSL/TLS encryption portals and/or secure VPN connections.

Entity Verification

- CHIS, Inc. staff undergo vigorous background checks and verification processes.
- Entry points to the CHIS, Inc. network and system are verified by network passwords and user names.

Transmission Security

CHIS, Inc. ensures transmission security to ePHI is in a manner that is in compliance with all state and federal guidelines regarding protection of patient health information HIPAA guidelines that pertain to Business Associates and the HITECH Act.

- **Integrity Controls**
- **Encryption**

Integrity Controls

CHIS, Inc. employs various layers of controls to maintain data integrity of not only ePHI, but also system and business critical data. To this end, there are backup procedures, authentication methods, auditing procedures, and intrusion detection mechanisms in place to safeguard all data residing on CHIS, Inc. network systems and offices. The following are methods employed by CHIS, Inc. for integrity controls.

- **Firewall blocks, audits, and detects intrusions on the edge network**
- **Threat protection with central management and auditing for system virus, spyware, intrusion detection and reporting**
- **Server backup and restoration following our Business Continuity policy**
- **Network auditing and management**

Encryption

CHIS, Inc. accesses client resources to access PHI on a daily basis. To safeguard the transmission of private information over public network infrastructures, all data communications are done over secure connections. Security and Encryption methods are in compliance and follow the guidelines set by the National Institute of Standards and Technology (NIST) on Information Security Publication 800-63. The following is a list of transmission security in use by CHIS, Inc.

- **Secure TLS/SSL webmail/exchange**
- **Secure IPsec VPN Site to Site connections**
- **Secure TLS/SSL client web portals**
- **Secure Multi User VPN clients for remote access**
- **Secure Cisco compatible VPN Clients**

Audit Control

CHIS, Inc. has in place audit controls to monitor activity on electronic systems that contain or use ePHI and in a manner that is in compliance with all state and federal guidelines regarding protection of patient health information that pertain to Business Associates and the HITECH Act.

Hardware and **software** systems are in place for regularly monitoring and reviewing of audit records to ensure activity on those electronic systems are appropriate. Such activities include, but are not limited to, logons and logoffs, file accesses, updates, edits, and any security incidents. Monitoring and review of audit trails are as close to real time as possible. There is no benefit to discovering a problem days or weeks after it has occurred.

Audit Procedures

CHIS, Inc. performs daily auditing of it's internal network and systems to make sure they are in compliance with our security policy.

- **Server audit reports**
- **Anti virus, spyware, intrusion and compliance audit reports**
- **Network vulnerability audit reports**
- **Network audit reports**
- **Web usage audit reports**
- **Systems and desk audits**
- **Client system audit reports**

Compliance

CHIS, Inc. is committed to compliancy with HIPAA and HITECH throughout it's business. The process of evaluating our policies and procedures to always be at the forefront of HIPAA and HITECH compliancy is ongoing. We provide continuing training to our workforce in HIPAA and HITECH. CHIS, Inc. HIPAA policies and procedures has demonstrated compliancy to confidentiality, integrity, and availability.