HIPAA Computer Compliance

While no vendor can make you HIPAA Compliant, Crystal PM has designed a checklist to meet key HIPAA standards with recommended office standards.

Equipment physical security
Theft of computer equipment is a leading source of data theft, including identity fraud and privacy violations.

- ☐ All computers are located in areas not easily accessible to outsiders.
- ☐ All employees lock doors and windows whenever the office is empty.
- ☐ Servers are physically secure in a separate area.

Access Security
Secure computing depends on ensuring that only authorized personnel can access office computers and data.

- ☐ Only authorized personnel have access to our computers.
- ☐ Require passwords for access to all workstations and servers.
- ☐ All computers are password protected.
- ☐ Computer left unattended for extended periods of time are logged off or need password verification.
- ☐ Users log off or shutdown computers at end of day.
- ☐ Computers not using secure operating systems have bios passwords.
- ☐ Passwords are periodically changed.
- ☐ Emphasize to all users that their password and user ID is private, and not to be written down or shared.
- ☐ Disallow dial in access to office computers without proper security measures.

Defensive Security
Computer viruses, Trojan horses, and hacking represent significant and growing threats to businesses. Data can be destroyed and personal information stolen.

- ☐ Anti-virus software is installed on all computers.
- ☐ All anti-virus software is the latest version.
- ☐ All anti-virus software is configured to detect email macros and viruses.
- ☐ If using Norton Anti-virus, are all computers set to "Enable File System Real-time Protection."
- ☐ All Microsoft Office macros and Visual Basic programs automatic executions have been disabled on all computers.
- ☐ Computer users never open attachments unless the attachment is expected.
- ☐ No computer desktops are configured to "View my Active Desktop as a web page." (It can generate virus contamination if visiting a web site that has a virus.)
- ☐ All computer users know what to do if their computer becomes infected with a virus.
- ☐ All computers with direct access to the internet have a private IP address or firewall.

Crystal Practice Management
11118 Conchos Trail * Austin, TX 78726 * Phone (866) 442-4142 * Fax (512) 335-8263

Operating System Security
The operating system software is the key to each computer's operation. It must be functional and up-to-date to establishing a secure computing environment.

- ☐ All computers have appropriate operating system software security patches installed.
- ☐ Operating System security patches and critical updates are regularly checked for and installed.
- ☐ We have disabled all unnecessary services and features in our desktop and server operating system configurations.
- ☐ We prohibit or restrict shared drives or folders on our desktop computers.
- ☐ We have verified that file permissions are properly set on our computers and our network.
- ☐ Auditing is enabled on all file servers for logons and file shares.

Application Software Security
The expanded features and increased complexity of applications such as word processing, e-mail, and web browsing create new security vulnerabilities.

- ☐ All computer applications are configured for security.
- ☐ Application software updates and security patches are identified and installed in a timely manner on all computers.
- ☐ Online orders are placed only through secure web sites.
- ☐ Each staff member has the appropriate level of access to software applications.
- ☐ Application access is promptly removed for employees who no longer need it.

Data Loss Security
Hardware can be replaced and application software reloaded from original media, but data recovery relies on systematic backup procedures.

- ☐ All computers and servers have appropriate data backup plans.
- ☐ Data backup plans are documented.
- ☐ All staff members know how to complete the recommended backups for the computers they use.
- ☐ Backup procedures include secure off-site storage.
- ☐ UPS (Uninterruptible Power Supply) systems are in place for all servers.
- ☐ Backups are periodically checked and evaluated for data verification.
- ☐ Backups are kept secure or encrypted.

Data Access Security
The Government mandates through law specific data access security and privacy requirements. Such sensitive data require protection against unavailability, unauthorized access, or disclosure.

- ☐ Only essential data is shared across the network.
- ☐ All locations of sensitive data records are known.
- ☐ All monitors are located out of unauthorized view.
- ☐ All printers and faxes are in a secure location and outside of patient view.
- ☐ Confirmation calls are placed for the phone number for all faxes that contain patient health information.
- ☐ Access to sensitive data is restricted on a clearance and need-to-know basis.

- ☐ All staff members are aware of what constitutes sensitive data.
- ☐ Unencrypted transmission of sensitive data or memos through e-mail is prohibited.

Disaster Recovery
Knowing how to react in an emergency will minimize the risk of damage and allow quick restorations of operations.

- ☐ We have a current inventory of our computer equipment, software, and critical data files.
- ☐ We have written documentation of each computer's CMOS, network, and security settings.
- ☐ Disaster recovery plans are in place due to system failures or data loss.
- ☐ Disaster recovery plans are documented.
- ☐ All staff are aware of what to do and whom to contact in case of a disaster.

Staff Awareness
The primary goal of computer security preparedness is to reduce security vulnerabilities through smart security practices.

- ☐ Is there a Privacy Officer or HIPAA Point Person (HPP) in charge of HIPAA compliance.
- ☐ Appropriate information and training about computer security is available to all staff members.
- ☐ All employees understand their personal responsibility for computer security.
- ☐ We have a written security policy and require all employees and users to read and sign it.
- ☐ Our security policies and procedures are completely documented.
- ☐ All computer users are aware of and agree to these policies and procedures.
- ☐ All staff are kept current on security issues and alerts.