hostmyehr

Health Insurance Portability and Accountability Act (HIPAA)

Statement of Compliance

hostmyehr.com has implemented many measures to help ensure that our services are compliant with the regulations and conditions set forth in the Health Insurance Portability and Availability Act of 1996 (HIPAA), subsequent amendments and HITECH. hostmyehr.com is committed to continually improving its available technology to become increasingly more secure and better capable of meeting the high demand of information access against the increasing demands for information security.

Administrative Safeguards (HIPAA 164.308)

hostmyehr.com has put processes and systems in place to provide for the appropriate assignment of access permissions to the appropriate persons. Actions are in place to govern the movement of our workforce and the privileges associated with those movements. Information security awareness training is a mandated event for all staff, as well as periodic reviews of contingency plans, audit trails, and security.

Physical Safeguards (HIPAA 164.310)

hostmyehr.com and its co-location data centers are physically secure. Access to the building, floor, and data centers are all independently controlled via card and centralized biometric system access, preventing walk-up intrusion, especially after hours. The data center is monitored 24 hours a day with video surveillance, advanced fire protection systems, uninterruptible power supply, and emergency power for all systems, including refrigeration. Annual reviews of the data center facility security plan, disaster recovery plan, and contingency plans are conducted by a certified and experienced third-party, according to SSAE-16 SOC 1, 2 and 3 standards. Specific security measures are in place in the facilities to guard against equipment disposal and reuse which may inadvertently compromise sensitive information.

Technical Safeguards (HIPAA 164.312)

hostmyehr.com complies with these regulations by utilizing varied audit controls, data integrity mechanisms, verified backups, entity authentication programs for all staff, and increasing measures to provide better data integrity and encryption. Additional safeguards include:

1. hostmyehr.com servers do not accept Anonymous-FTP connections, nor in fact any FTP connections from the outside world at all, the most common hacker method of seeking out an FTP site for possible attack.
2. A username and password generated by the Covered Entity is required to access PHI. Important Note – Password creation is the responsibility of each Customer, and neither hostmyehr.com nor any other Customer is granted access to those passwords. hostmyehr.com recommends that Customers make all passwords difficult to crack, plus follow reasonable standards for password security. Customers may contact hostmyehr.com through the support portal on the web site for recommendations.
3. hostmyehr.com offers the use of 128-bit transfer encryption.
4. hostmyehr.com proactively monitors and reacts to intrusion attempts into its systems through the use of a sophisticated Intrusion Detection System (IDS) and multiple operating system-level security tools.
5. No copies of PHI files reside on any offsite or long-term storage media.
6. The exception to #5, above, is that when services are discontinued with hostmyehr.com, the data is encrypted and made available in a secure manner to the Customer for a designated period of time. It is then deleted and destroyed, in keeping with HIPAA guidelines. No printed reports or paper copies are ever retained by hostmyehr.com. In addition, all retired computers and storage media, such as flash drives and hard drives, are destroyed according to proper HIPAA guidelines.
7. hostmyehr.com staff are trained about HIPAA and security awareness procedures. Confidentiality agreements are signed by hostmyehr.com staff, and security procedures are implemented when any hostmyehr.com staff terminates employment.
8. hostmyehr.com deploys a multi-layered data backup strategy, to allow recovery for Customers, if necessary, consisting of the following:

- Continuous real-time backup between hard drives in redundant arrays in each server
- Continuous real-time offsite backup to a mirrored node in a separate geographic location
- Nightly byte-level backups to 24-hour staging servers
- Nightly byte-level backups from the staging servers to long-term archive servers with data versioning
- Replication between two geographically distinct data centers