Bank on MedicalBillingStar for Round-the-clock HIPAA

Our Tension-free HIPAA Compliant Services

TOLL FREE
1-877-272-1572

MEDICAL BILLING STAR
" The EMR Billing Specialists "

Neurological Servers Rendered "hors de combat"

During unsuspecting "wee hours" on a holiday, a frantic call from Gloria Edwards, CEO of San Francisco-based Starbuck Clinic, galvanised the 24x7 "Rapid Action Force" of MedicalBillingStar into prompt action. Servers hosting EMR services at Starbuck, a 500 bed neurological clinic, were hacked and disabled, rendering the clinic non-functional.

Swift Evaluation, Analysis, and Action

An in-depth study by MedicalBillingStar revealed 4 problem areas:

Disruption of EMR: The servers were subject to denial of service (DOS) attack, thus disrupting the EMR services.

Email vulnerability: Inter-doctor and intra-clinic email messages relating to patients were transmitted on public internet-based email services - Yahoo, AOL, etc. These emails were not encrypted. There was no business associate (BA) agreement on Health Insurance Portability and Accountability Act (HIPAA) compliance between email vendors and the clinic.

Nothing to fall back! Back up storage of patient health information (PHI) as a contingency plan was not catered for.

Circumspection is a must: Secured storage, processing, and transmission of PHI were not ensured.

The Path to Salvation

Embarking on a corrective action plan on top priority, MedicalBillingStar guided Starbuck clinic implement 15 life-saving measures for HIPAA compliance:

Incorporate the administrative and technical security policies and procedures for protection of PHI.

Clinical workflows were also imbibed in the procedures.

Provide proactive and continual on-going education and training of the clinical staff in state-of-the-art privacy and security techniques to counter hacker threats in stealing of confidential PHI.

The watchdog: Appoint a security team for round-the-clock monitoring of PHI security and privacy, as well as reporting of breeches and corrective actions, as mandated by HIPAA.

Do not take it for granted: Periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its PHI, and initiation of corrective measures.

No to stealers! Encrypt data files using validated cryptographic modules. Implement encryption procedures to cover the following;

Patient billing and administrative information exchanged with payers and health plans.

Utilization and case management data, including authorizations and referrals that are exchanged with payers, hospitals and utilization management organizations.

PHI displayed on a Website or portal.

Lab and other clinical data electronically sent to and received from outside labs.

Word-processing files used in transcription and other kinds of patient reports that are transferred electronically.

Do not overlook confidentiality aspects in mobile phones used by the clinic and patients, which contain PHI. Secure PHI by using encryption program for mobile devices. This does not tantamount to over-ensuring.

Secure transmission media: Transmit PHI over secure media to bill Clearinghouses, outsourced medical transcription, coding and billing services, and insurance companies.

Securing emails also: Desist from using the public domain email system. Use secure email system among the doctors, between clinic and patients, and between the clinic to bill clearing houses, insurance agencies, and outsourcing vendors. This ensures confidentiality of PHI.

Audit go-ahead: Appoint an independent auditor to periodically approve the clinic's incorporation of the HIPAA omnibus rule.

Easy-to-handle medical audits: Identify and implement software system to manage medical claims audits.

Access control: Restrict access to PHI to obviate fraud and wrongful disclosure.

Device and physical security: Incorporate action plan to counter physical loss or theft of phones used by doctors and patients, which contain PHI (disabling the phone, etc.)

Exigency plan: Create secure back up storage facilities for PHI.

Transactions and Code sets: Use standard content, formats and coding, and eliminate use of duplicative and local codes, as required by HIPAA law related to medical transactions and standard medical code set standards.

Automation tools to reduce waste and save time: Use physician's automation tools such as the one for eligibility verification. According to American Medical Association (AMA) such tools help to save physicians and health insurers nearly $30 billion per year.

On-the-toes with Anti-complacency Warnings

MedicalBillingstar follows it up by giving regular updates to the clinic on live recent examples of how lackadaisical approach to HIPAA compliance has resulted in stiff penalties such as:

$1.7 million HIPAA penalty for violations: WellPoint, which serves nearly 36 million people through its affiliated health plans, was fined $1.7 million for potential violations of the privacy and security rules under the HPPAA.

$400,000 penalty for exposing information on Website: Idaho State University has agreed to pay $400,000 due to an incident that could have exposed information on 17,500 patients at the university's Pocatello Family Medicine Clinic site.

$1,500,000 penalty for theft of hard drives: In March 2013 U.S Department of Health and human Services and Blue Cross and Blue Shield of Tennessee was fined $1,500,000, due to potential HIPAA

By rapidly implementing HIPAA compliance measures, MedicalBillingstar has justified its nickname of "Rapid Action Force", which has been coined by our satisfied and happy medical clients across the US. This unique case has emerged as a role model across the US and emphasises the importance of speedy and reliable implementation of HIPAA compliance for the medical fraternity.