TOP 5 TAKEAWAYS FROM HIPAA OMNIBUS AUDITS

With the recent changes to the HIPAA Omnibus Rule, organizations and their business associates must address how they're compliant and what changes to make to minimize risks. The Omnibus Rule creates urgency for clinicians and administrative staff to use a HIPAA compliant secure messaging system. Sharing PHI over mobile devices requires more security than a standard SMS service offers.

When selecting a vendor, it is important to ensure that any solution for communicating or storing PHI is properly documenting each exchange, in case of an audit. Worried about your organization and clinician staff not staying compliant? Assess the security of your organization's exchange of PHI with these Top 5 best practices to avoid unexpected fines or mistakes during a surprise HIPAA audit.

tigertext

TOP 5 TAKEAWAYS FROM HIPAA OMNIBUS AUDITS

1. WATCH OUT FOR FALSE CLAIMS OR PROMISES

Make sure the vendor you are using to exchange PHI uses a secure messaging system. Don't fall victim to false claims that promise HIPAA compliance.

2. CONTROL INTERNAL PROCESS CHANGES

Track organizational changes and keep detailed records of the evolution of operational processes. Even the smallest internal change could impact the way your clinical staff exchanges sensitive material.

3. CONSISTENTLY USE SECURE COMMUNICATIONS

Be a HIPAA compliant secure messaging advocate. Stress the fact that all staff members must utilize secure messaging when sending confidential information on mobile devices.

4. DON'T ASSUME YOU'RE SECURE

To avoid future fines that could happen during a surprise audit, conduct periodic risk assessments of your organization's security and stay up to date on any changes in versions or updates your secure messaging vendor makes. This could save you thousands of dollars in the long run.

5. ALWAYS MAKE PATIENT CONFIDENTIALITY A PRIORITY

Put your feet in your patients' shoes. Nobody wants their personal health information out in the open. Breaches and hacks happen constantly. Stress the importance of using these best practices to avoid any private information being leaked.

With the increase of mobile devices at work, it's necessary to guarantee that mobile device usage meets HIPAA compliance standards and guarantee that all PHI remains confidential. Implementing a secure messaging system can help your organization ensure that all PHI sent or received among employees remains confidential and HIPAA compliant — protecting the privacy of your patients. With these Top 5 takeaways, you can help ensure your organization never falls victim to a HIPAA Omnibus audit.