IntakeQ

Your Daily HIPAA Compliance Checklist

This is an extra resource to go along with the original article:

The Most Common HIPAA Violations and How to Prevent Them

❑ I have checked the U.S. Department of Health and Human Services for announcements of updates or changes to HIPAA and the PPACA.

❑ Any information to be destroyed from the previous day has been shredded.

❑ I have responded to all appropriate requests for patient information from yesterday.

❑ I dealt with any employees/staff who were caught speaking about patients in inappropriate settings.

❑ My team or I did not leave any medical information in public places.

❑ Any patient information I disclosed was accompanied with a medical release form with the correct information and date.

❑ All paper documents are accounted for.

❑ All paper documents from the previous day have been converted to electronic records.

❑ My staff is trained to resist phishing and social engineering attacks.

❑ A security IT firm is monitoring my record system for vulnerabilities and threats.

❑ I use encryption on my data at rest and in transit.

❑ My computer systems are equipped with malware blocking software.

❑ Every vendor I use is a certified HIPAA business associate and I have a proper business associate agreement with them.

❑ All devices/software are equipped with two-factor authentication, well-crafted passwords and encryption.

❑ Any transportable devices are locked away at the end of the day.

❑ I have a policy in place for regular compliance training for my staff.

❑ I am confident that my staff is properly trained to prevent HIPAA violations.

❑ Unauthorized personnel are restricted from accessing physical or electronic records.

❑ Policies are in place to limit who uses workstations.

❑ All of my emails to patients are compliant.

❑ There is a contingency plan in place to continue operations if there’s a disaster (such as an information breach).

❑ I have properly reported any security incidents.