HIPAA Privacy and Security

HIPAA Compliance

Let's Get YOU on the HIPAA Compliance Journey today!

Tel: 888 444 9995 – www.xTerraLink.com

IT HIPAA Sample Checklist

Access Control	• Have access needs of the Practice's users been evaluated in relation to their job roles • Have access been granted to those authorized persons, or software programs or hardware that have been authorized access • Are there unique name and/or number for identifying and tracking user identity • Can the System activity be traced to a specific user • Has the necessary data been made available in the System logs to support audit and other related business functions • Has there been terminations, additions, changes to users, hardware, software, generic user IDs, emergency access • Has encryption process has changed
Audit Control	• Review audit logs for suspicious activities or unauthorized access
Password Control	• Has authentication controls (passwords, etc.,) been reviewed for process or technology changes and been documented
Work-station Use	• Has WS been identified, and added to asset inventory • Have Privacy Screens been added • Have WS been removed or added and how is the disposal process • Have WS been updated with users roles and functions

Work-station Security	• Has Workstation physical access been changed • Has workstation inventory been kept up to date • Has workstation physical security (cameras, doors, cable locks, etc.,) been added or changed • Are devices (mobile or smart phones, laptops, hard disks, etc.,) been updated with security (e.g., passwords, hard disk encryption, privacy screens, etc.) • Are devices been loaded with anti-malware or virus scan and be configured to update automatically
Device and Media Control	• Are off-site ePHI exact copies of original ePHI • Is ePHI stored in a secure off-site location and transported safely • Is off-site location equipped with protection (fire protection, fire suppression systems, fireproof safe, etc.) • Has data restoration been tested for integrity
Data Backup and Recovery	• Has backup process been changed since the last process • Has the software and the hardware been reviewed for operational integrity (systems and devices in working condition) • Is the status of the IT operational documentation up to date • Has the business continuity process changed