HIPAA Considerations for your On-Premise Telephone System

Organizations required to comply with the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) expand beyond the medical industry today and now include many service providers for the medical industry known as business associates. Whether your organization is a covered entity, such as a health plan, a health care provider or a health care clearinghouse, or a business associate, finding business solutions, including telephone systems such as your on-premise telephone system, that help your organization comply with HIPAA is vital to your success.

At Toshiba, we know that all on-premise telephone systems are not the same. Investing in the right on-premise IP or converged telephone system technology for your organization can help with the ongoing management of compliance with HIPAA’s privacy and security requirements, with the goal of avoiding liability under HIPAA in the future.

There are many means to reach the end goal of HIPAA compliance. An organization may assess reasonableness of different means based on factors such as the size and complexity of the organization, the organization’s technical infrastructure and capabilities, the costs of the means and the probability and criticality of potential risks to the patient information (PI).

HIPAA requires organizations with PI to ensure the confidentiality, integrity and availability of all PI in electronic form; to protect against reasonably anticipated threats to the integrity or security of the PI; to protect against reasonably anticipated threats of non-permitted uses of the PI; and to ensure that the organization’s workforce is in compliance with HIPAA’s security rule. HIPAA security compliance requirements are typically broken down into 3 main categories:

**Administrative Safeguards.** An organization must continuously assess the risks to its data. This includes identifying information systems that create, receive, transmit or maintain PI in electronic form as well as the individuals who have access to these systems. The ultimate effectiveness of an organization’s safeguards depends in large part on the policies it adopts, implements and enforces with respect to the storage of and access to PI.

**Physical Safeguards.** The ways in which data are used and stored are constantly changing – evolving to meet the many needs of our world, especially frequently changing government regulations. Making sure that appropriate physical safeguards, from doors to locks, are maintained is an important step toward ensuring HIPAA compliance. This includes securing telephone lines, telephone systems and related software from unauthorized physical incursions. Policies that limit physical access and entry through the use of doors, cabinets, closets, and
gateways with keys or passcodes access can greatly enhance an organization’s ability to achieve HIPAA compliance.

**Technical Safeguards.** Just as the ways data is used evolves, so do the threats to that data. HIPAA compliance requires adequate use of technical safeguards. For example, unique user identification and authentication are among the few specified technical requirements under HIPAA’s security rule. Security of voicemails can be enhanced through the use of passwords and other authentication measures designed to ensure that access and use are limited to authorized users. Strong password policies, firewalls and intrusion detection for telephone lines and anti-virus software are all technical solutions available to safeguard PI.

HIPAA compliance requires a comprehensive approach. Toshiba understands the need for covered entities and their business associates to protect PI that may be stored on, or transmitted by, Toshiba’s on-premise IP or Converged Telephone Systems.

While being user friendly and efficient, Toshiba’s on-premise IP Telephone Systems retain all data on the organization’s internal system, and provide many security mechanisms. Toshiba uses SSLV3 secure access to the web browser to gain access to the systems. Control of system administration and tracking of administrative activities are provided for via multi-level system administration password protection options.

Identity management and access control are provided for at the voicemail, VoIP handsets and software client levels. In addition to passwords, users taking advantage of voice via the UCedge Unified Communication application are automatically logged out once a new device has been activated for voice.

Additionally, at a physical level, Toshiba’s on-premise IP Telephone Systems contain a locking bezel mechanism restricting the ability to download or control the system without authorization.

Toshiba’s on-premise IP or Converged Telephone Systems provide solutions to health care providers.

http://www.telecom.toshiba.com/Telephone_Systems_Resources/Success_Stories/#healthcare

For more information on HIPAA guidance and best practices, go to the United States Department of Health and Human Services website: [http://www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/)