HIPAA Brief www.semelconsulting.com

Why Technology Manufacturers, Service Providers, Help Desks & Managed Service Providers must comply with HIPAA

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) requires that electronic Protected Health Information (ePHI) be secured against loss or unauthorized access.

Business Associates

In 2003 HIPAA defined health care providers and payers as *Covered Entities*. Organizations that support Covered Entities and come in contact with Protected Health Information (PHI) are *Business Associates,* even if they never access specific patient records. Business Associates include computer service providers, printer and copier service providers, Managed Service Providers, lawyers, accountants, collection agencies, shredding companies, and many other businesses that support health care organizations.

The following are all Business Associates:

- IT manufacturers that offer installation, warranties, and repairs of devices with hard drives that may contain ePHI
- OEM service organizations, contract service partners and authorized service providers – whoever may provide service
- Logistics companies that handle warranty returns, lease returns (of hard drives or devices that include drives)
- Data recovery specialists
- Equipment disposal companies
- Organizations that provide Help Desk services where technicians may open remote sessions with end-users
- Companies offering online backup; data center hosting or colocation; or Cloud Services that include data storage

Business Associates have caused many data breaches but were out of the reach of the federal HIPAA enforcement agencies. Business Associates signed agreements stating they would protect patient data, but there was no government enforcement. The HITECH Act of 2009, a law best known for funding Electronic Health Records for doctors and hospitals, requires Business Associates to comply with HIPAA and be directly liable for HIPAA penalties. This actually *increases* the liability for Covered Entities who now will share liability with Business Associates and their subcontractors. *Enforcement of the Final Rule will begin September 23, 2013.*

HIPAA Omnibus Final Rule

In January the Department of Health & Human Services (HHS) released the HIPAA Omnibus Final Rule, setting specific compliance requirements for Business Associates. *Compliance is not just a legal exercise. It means more than just signing Business Associate Agreements. Business Associates are required to implement HIPAA-specific policies & procedures, perform a HIPAA risk analysis, train their workforce, and deliver and document HIPAA-compliant services. Everything must be in place by September 23, 2013.*

"This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented," said HHS Office for Civil Rights Director Leon Rodriguez. "These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

Subcontractors

The Final Rule requires Business Associates to ensure that all of their downstream Subcontractors will comply with HIPAA by signing Business Associate Agreements and implementing HIPAA compliance programs, including HIPAA-specific written policies and procedures; workforce training; a HIPAA risk analysis; delivery of HIPAA-compliant services; and documenting their work with enough detail to sustain a HIPAA audit or data breach investigation. *If a Business Associate shares protected data with anyone that does not comply with HIPAA, it is a data breach requiring notifying their health care client, who must then notify patients and the federal government. Penalties of up to $ 1.5 million per occurrence may apply, plus costs to notify patients, legal fees, and reputational damage control costs.*

Organizations that Maintain Data

The Final Rule also requires that any person or entity that 'maintains' (stores) protected data, *even if they don't look at it*, is a Business Associate. Notable was that there is no exemption for encrypted data, data protected by password, data in locked cabinets where the owner of the facility does not have keys, or other situations where the data is not— or cannot be— accessed. The Final Rule discusses this starting on page 24 https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf.

Where can I get more information?

HIPAA Business Associates: Myths & Facts
US Dept. of Health and Human Services Understanding HIPAA Privacy

www.semelconsulting.com
888-997-3635 x 101

Semel Consulting works with IT resellers and vendors to develop HIPAA compliance programs. Don't rely on your staff to develop a HIPAA compliance program that will sustain an audit. Work with your lawyers to develop a Business Associate Agreement for your clients/ partners/ resellers and any subcontractors you work with. Work with Semel Consulting to develop written HIPAA policies, procedures, a risk analysis, and a plan to ensure HIPAA compliance on an ongoing basis.