Why Data Centers, Cloud vendors, and Online Backup Providers have to comply with HIPAA

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*. Business Associates caused many data breaches but were out of the reach of the federal HIPAA enforcement agencies. They signed Business Associate 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.

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. Two sections in the Final Rule affect IT VARs/MSPs and their vendors that provide them with data center hosting, colocation, Cloud services, and online backup. *Compliance means more than signing Business Associate Agreements. Business Associates are required to implement HIPAA-specific policies & procedures, have a HIPAA risk analysis, train their workforce, and deliver and document HIPAA-compliant services.* Enforcement of the Final Rule will begin September 23, 2013.

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 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. Since PHI could come from a Covered Entity or Business Associate, it is virtually impossible for a hosting, cloud, or backup vendor to prevent it from entering their system. This presentation (by lawyers from the HIPAA enforcement agency) provides info on Slides 9 and 10. http://csrc.nist.gov/news_events/hipaa-2013/presentations/day2/kenney_holtzman_day2_1030_hipaa_hitech_rule_changes.pdf

This article is important because it references a presentation by Leon Rodriguez, the government's chief HIPAA enforcer, who clearly says that data centers offering colocation and hosting now have to comply.
http://healthworkscollective.com/onlinetech/87816/himss-13-hhs-final-ruling-changes-rules-roles-hipaa-hosting

SSAE-16, SOC-2, or SOC-3 do not mean you are HIPAA compliant

There are different compliance requirements, from different organizations and agencies, and they are not interchangeable.

This article from datacenterknowledge.com addresses the idea that compliance can be mixed between requirements. Note that the article was written before the Omnibus Final Rule but has some valuable information comparing various accreditations.
http://www.datacenterknowledge.com/archives/2012/06/29/hipaa-compliant-data-centers/

This reader's comment is also relevant.

> *Certainly **SOC 2** brings a somewhat better level of objectivity to data center audits than SSAE 16 (SOC 1), but it **is not a substitute for a HIPAA audit. HIPAA requires specific policy, personnel training and breach remediation processes that are not covered in SOC 2 audits. In addition the HIPAA security rules are very different than SOC 2 standards.** We support 4 different audits for each of our data centers: SSAE 16, SOC 2, HIPAA and PCI. Each audit has its own purpose and own requirements. **While SOC 2 helps data centers move towards a more objective audit, it's not a substitute for HIPAA or a PCI audit.***
>
> ***You can bet that HHS isn't going to accept SOC 2 as a proxy for HIPAA compliance when it comes to penalties associated with PHI breaches.***

Where can I get more information?

HIPAA Business Associates: Myths & Facts
Cloud Storage Providers Storing Protected Health Information May Be Obligated to Comply with HIPAA

SEMEL CONSULTING
www.semelconsulting.com

Semel Consulting works with IT resellers and their vendors to develop HIPAA compliance programs.