Four Myths about Security Compliance That Every IT Pro Needs to Know

As data breaches become more frequent, security and compliance issues are becoming the cornerstone of information security. What do you need to know about the different certifications?

Myth #1 Only hospitals and insurance carriers need to worry about HIPPA.

Why you care about HIPAA[1]?

Because you trust health care providers to protect your privacy. Private health data is exposed to dozens of different organizations in today's healthcare systems.

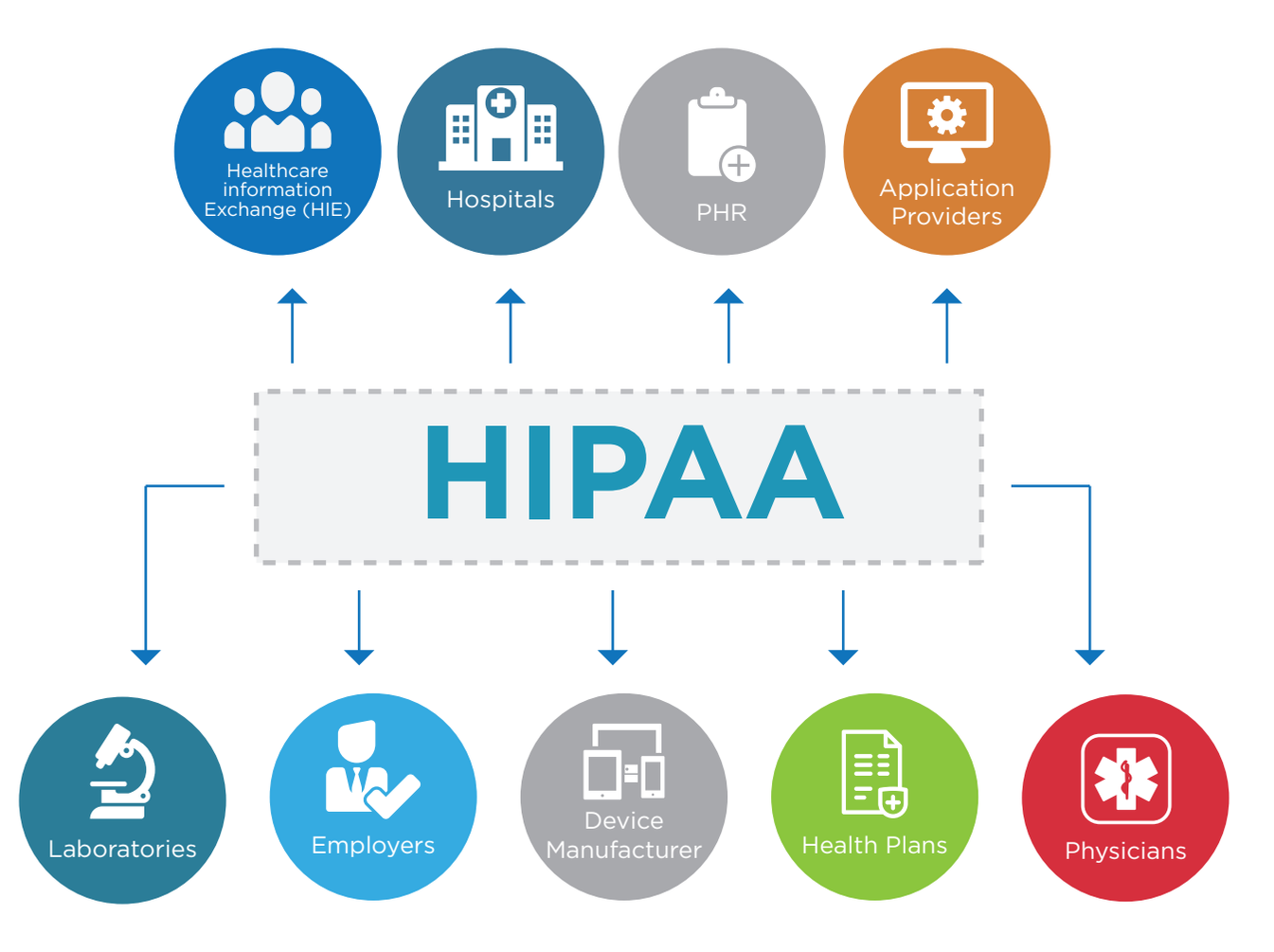
Goal of HIPAA – Protecting personal health information Perfect Storm is fuelled by increasing:

- ↑ Numbers of Data Breaches (2 major insurance carriers were hacked in 2015 resulting in the largest healthcare data breaches in history
- ↑ Costs of HIPAA violations

FACT: Simple mistakes can equal big fines. Even small practices must comply.

HIPAA Health Insurance Portability & Accountability Act

As the number of providers increases – so do the risks of failure:



Myth #2 Only Large Online Retailers need to worry about PCI DSS

Why you care about PCI DSS[2] Compliance

Because online customers put trust in you every time they make a purchase
Goal of PCI DSS is to process online payments securely

The Truth is: According to the PCI Security Standards Council, if your business registers **one** credit card transaction or **six million**, you must be compliant. Businesses are liable for the credit card data of their customers and can face penalties of up to **$100,000** for each violation

The statistics are alarming:

80% of Companies are failing PCI validation assessments in 2014 (Verizon PCI Compliance Report)

45% of Americans report they have been notified that their credit card information has been stolen in a breach.

69% of consumers are less inclined to do business with a breached organization (Quirks Radius Global Marketing Research, 6/14)

Myth #3 Only public companies need to worry about financial control compliance like SSAE 163 SOC 1[4], SOC 2[5] and ISAE 3402[6]

These reports demonstrate your company is accountable for the secure handling of data in order to protect the public from accounting errors and fraud. Adherence to the guidelines is becoming increasingly important as companies move to the Cloud or SaaS models where sensitive corporate data is held by third parties.

SOC 1

- Internal controls over financial reporting
- Used by User's auditors and users' controller's office

SOC 2

Security
The system is protected against unauthorized access (both physical and logical

Availability
The system is available for operation and use as unauthorized or agreed

Processing Integrity
System processing is complete accurate timely, and authorized

Confidentiality
Information designated as confidential is protected as committed or agreed.

Privacy
Personal Information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entities privacy notice

Used by Management, regulators & other. Shared under NDA

How are SSAE 16 and ISAE used?

A service provider can undertake its own SSAE 16/ISAE-3402 assessment, and provides copies of the auditor's report to their customer's auditors upon request. Because it's an "auditor-to-auditor" report, a customer's auditors rely on the report to verify the quality of your company's controls without assessing them directly.

The Truth about SSAE 16 and ISAE 3402 Compliance

1. Required to perform outsourced services for Public Companies
2. Proves your company can be trusted to handle data of your clients
3. 3rd party review of your control and activities ensure they are functioning properly
4. It is required in many RFPs

Myth #4 All Data Centers offer Certified Compliant Solutions

The Truth is that few data centers offer compliant solution across multiple locations although the services they offer are fundamental to achieving security compliance.

365 DataCenters

100% COMPLIANCE

365 Data Centers is the first national colocation provider to achieve compliance with several of the most stringent industry standards across 100% of its facilities nationwide.

365 DATA CENTERS IS CERTIFIED FOR:

HIPAA | PCI DSS COMPLIANT 3.0 | SSAE 16 CERTIFIED TYPE II | ISAE 3402

systems | operational processes | security measures

For 365 to successfully pass the certification audits, it needed to present a consistent environment, operational framework and measures across all of its facilities.

> *"Certifying compliance across all facilities is a significant accomplishment and an uncommon feat these days. 365 continues to raise the bar for client services."*
>
> **Scott G. Price, CPA/CISA/CIA, Managing Director, A-lign**

365 DataCenters

About 365 Data Centers

365 Data Centers connects carriers, content publishers, cloud providers and their customers, at the edge, in a media-rich world. Through its 16 U.S. data centers, 100% uptime SLA, and national network of carriers and content providers, 365 Data Centers offers colocation and cloud solutions that are tailored to meet the needs of its customers. For more information, visit 365datacenters.com

1. Health Insurance Portability and Accountability Act
2. Payment Card Industry Data Security Standard
3. Statement on Standards for Attestation Engagements
4. SOC 1 Service Organization Control audits regarding internal control over financial reporting
5. SOC 2 are Service Organization Controls Reports audits to evaluate controls around security, availability, processing integrity and privacy
6. International Standards for Assurance Engagements a global standard for reporting on controls at service organizations in response to Sarbanes-Oxley Act