webair
Secure. Managed. Scalable.

HIPAA COMPLIANT

# HIPAA Compliance:
## Protecting Electronic Health Information

In the world of Health Information Technology (HIT), **privacy** and **security** are key pillars to effectively serving patients and avoiding **costly data breaches**.

**142.8M** people in the U.S. have been affected by publicly reported HIPAA breaches in the last 6 years
*- Department of Health and Human Services*

From 2009 to 2014, HIPAA data breaches climbed **138%**
*- Redspin*

Data breaches cost an estimated average of **$3.5M**, while the total annual cost for the industry as a whole is estimated at **$5.6B**
*- Department of Health and Human Services' Office for Civil Rights*

2015 healthcare data breaches passed the **100 incident** milestone in the first **5 months**
*- Department of Health and Human Services' Office for Civil Rights*

As **data breaches** and **cybercrime** advance rapidly, taking every precaution to safeguard ePHI as well as patients' rights and protections is **critical**.

Cyber criminals are selling medical information on the black market at a rate of **$50** for each partial EHR, compared to **$1** for a stolen social security number or credit card number
*- Mediscape*

The annual economic impact of medical identity theft is **$30.9B**
*- The Ponemon Institute*

So far in 2015, patients file an average of **1,500** HIPAA complaints per month
*- Department of Health and Human Services' Office for Civil Rights*

**Avoid HIPAA violations** by choosing a HIPAA-compliant managed infrastructure provider to make the adoption and expansion of healthcare IT solutions **safe**, **secure** and **reliable**.

**83%** of healthcare organizations use cloud-based apps
*- HIMSS Analytics Survey*

Healthcare companies will invest **$12.6B** in cloud computing by 2020
*- Persistence Market Research*

**73%** of healthcare organizations are not confident that their partners would be able to detect or notify them in the event of a data breach
*- Information Security Media Group*

Ensuring data centers and managed services are **HIPAA-compliant** helps guarantee that providers' sensitive electronic Protected Health **Information** is **safe** and **secure**.

**55%** of healthcare providers do not regularly train staff on proper security protocols
*- The Ponemon Institute*

Under the HIPAA Final Omnibus Rule, business associates responsible for violating HIPAA privacy & security rules face up to **$1.5M** in annual fines
*- Department of Health and Human Services' Office for Civil Rights*

# The Do's & Don'ts of HIPAA Compliance:
## Remain Vigilant, Remain Secure

### Don't

**Don't** allow your healthcare organization or its patients to become casualties of costly data breaches or cyber crime.

**Don't** assume that your provider has achieved stringent data center and service certifications, including SSAE 16 SOC 1 TYPE II, PCI DSS and HIPAA Matrix.

**Don't** assume that your infrastructure is wholly controlled and monitored by your provider. Many leave the management up to you.

**Don't** wait to update and educate your staff on the specific provisions of HIPAA compliance.

**Don't** assume that a HIPAA violation can only occur after a data breach. In addition to security, HIPAA also requires that data is available and intact. A company can be in violation of HIPAA if a system is down or inaccessible, or if data is unavailable due to corruption.

### Do

**Do** verify that your managed infrastructure provider or Business Associate is HIPAA-compliant and secure across all of its managed services, including Colocation, Bare Metal Servers, Public and Private Clouds, Cloud Storage and IP Transit.

**Do** confirm that your managed infrastructure provider or Business Associate undergoes data privacy and security audits that are performed and evaluated annually by an independent, third-party auditor, and that their HIPAA infrastructure is reviewed by an experienced HIPAA Compliance Specialist.

**Do** inquire if your managed infrastructure provider signs Business Associate Agreements (BAAs) with all of its healthcare customers, and if the company has ever experienced a HIPAA-related incident.

**Do** have the redundancy in place to ensure data availability, and the Disaster Recovery and Backups in place to ensure data integrity.

BROUGHT TO YOU BY

webair

Owning HIPAA compliance from the physical data center to the edge network

**www.webair.com/healthcare**