





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.



publicly reported HIPAA breaches in the last 6 years - Department of Health and Human Services



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



climbed 138% - Redspin



incident milestone in the first 5 months - Department of Health and Human Services' Office for Civil Rights

taking every precaution to safeguard ePHI as well as patients' rights and protections is critical.

As data breaches and cybercrime advance rapidly,



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 - Medscape



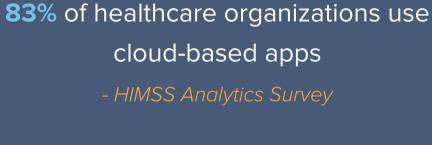
- The Ponemon Institute



to make the adoption and expansion of healthcare IT solutions safe, secure and reliable.

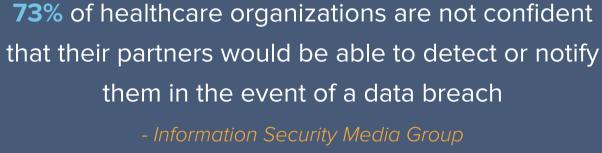
Avoid HIPAA violations by choosing a

HIPAA-compliant managed infrastructure provider







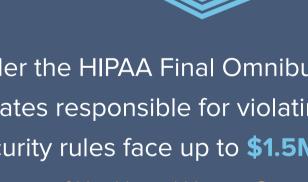


Ensuring data centers and managed services are HIPAA-compliant helps guarantee that providers'

sensitive electronic Protected Health Information is

safe and secure.





55% of healthcare providers do not regularly train Under the HIPAA Final Omnibus Rule, business staff on proper security protocols associates responsible for violating HIPAA privacy & security rules face up to \$1.5M in annual fines - The Ponemon Institute - Department of Health and Human Services' Office for Civil Rights

Don't

The Do's & Don'ts of

HIPAA Compliance:

Remain Vigilant, Remain Secure

stringent data center and service certifications, including SSAE 16 SOC 1 TYPE II,

Don't assume that your provider has achieved

Don't allow your healthcare organization or its

patients to become casualties of costly data

breaches or cyber crime.

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

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.

occur after a data breach. In addition to

Do confirm that your managed infrastructure provider or Business Associate undergoes data privacy and security audits that are

Cloud Storage and IP Transit.

provider or Business Associate is

Do verify that your managed infrastructure

HIPAA-compliant and secure across all of its

Metal Servers, Public and Private Clouds,

managed services, including Colocation, Bare

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.



Owning HIPAA compliance from the physical data

www.webair.com/healthcare

center to the edge network