

IS YOUR SENSITIVE PATIENT DATA SAFE AND SECURE IN THE CLOUD?

HIPAA-COMPLIANT SOLUTIONS FROM MEDICUS IT.



HIPAA regulations concerning the handling of a patient's Electronic Protected Healthcare Information (ePHI) create record-keeping and storage challenges for any healthcare organization. While the data must be secured according to stringent standards, it must also remain immediately accessible to authorized medical personnel in the course of administering critical care. With the advent of the cloud, data storage and backup providers now share responsibility for the protection of sensitive patient data from the very real threat of theft, mishandling, and misuse. Because patient privacy is at stake, federal law requires data storage and backup providers to implement physical security and electronic security measures that specifically protect ePHI. In addition, cloud solutions providers are responsible for immediately notifying patients if the ePHI storage is ever breached—a costly process in its own right.

Example of Breach: Compromised EMR

[Information Breach](#) [PHI Notification](#)
10,000 patients X \$50 per patient = **\$500,000**

Does your current data storage or backup provider have \$500,000 to cover the notification expense? If not, do you?

IS YOUR CURRENT CLOUD PROVIDER HIPAA-COMPLIANT?

Many data storage and backup providers do not comply with HIPAA's physical and electronic standards in their data centers, nor do they have the financial means to perform the required notifications in the event of a data breach. This creates a huge problem for healthcare providers, because they can be held liable for their data storage/backup service provider's data breaches or security lapses that compromise patients' ePHI.

Compliance with HIPAA requires that cloud solutions be verified by third-party audits to ensure the required levels of data protection and secure access are met. If your provider's data center and solutions have not been audited by a recognized third-party, then your provider is not in compliance...period.

OUR EXPERT HEALTHCARE SOLUTIONS ARE HIPAA-COMPLIANT

Healthcare providers rely on us for our experience with data storage and backup compliance. Our infrastructure—with redundant Cisco, VMware, and NetApp architecture—resides in two (2) fully-audited, HIPAA-compliant, Tier III data center environments, ensuring the deepest layers of fail-proof security and access available.

To prepare for the worst-case scenario, we've also invested in specialized insurance policies to cover the costs associated with an ePHI breach and the required notifications of such breaches. With Green Cloud's HIPAA-compliant data storage and backup solutions, your infrastructure is always insured against sensitive patient data breaches. *

*Green Cloud will only cover failures or breaches of Green Cloud infrastructure due to negligence on the part of Green Cloud.

Nearly 91 percent of healthcare organizations have experienced a healthcare data breach within the past two years alone, resulting in the loss of tens of millions of patient records.* It is incumbent on healthcare providers to invest in secure HIPAA-compliant cloud solutions to mitigate the risk of data breaches and avoid the costs that such a loss of confidential patient information can incur.

* <http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf>

678-495-5900 | www.medicusit.com

VIRTUAL SERVERS | DISASTER RECOVERY | BACKUP | VIRTUAL DESKTOPS

