COSMOS
Navigate the Compliance Universe

Compliance Today - March 2023

Narendra Sahoo (sahoonarendra507@gmail.com) is the Founder and Director of VISTA InfoSec, a global Information Security Consulting firm based in the United States, Singapore, and India.

Disaster recovery plan for HIPAA

By Narendra Sahoo PCI QSA, PCI SSFA and SLCA, CISSP, CISA, CRISC

HIPAA compliance is a requirement for every covered entity and business associate in the healthcare industry. All the healthcare organizations and service providers who come under HIPAA compliance are expected to meet the requirements and ensure compliance. The data privacy regulation is about securing the protected health information (PHI) through its outlined Security and Privacy rules. There are many aspects to meeting the requirements and achieving HIPAA compliance. Among all the requirements, the HIPAA Security Rule highlights the need to secure PHI data. The HIPAA Security Rule 164.308(a)(7) identifies the contingency plan[1] as a standard under HIPAA's Administrative Safeguards.

The contingency plan addresses the availability security principle related to recovering any kind of business disruption. This could be in terms of having access to information and critical systems when required. The contingency plan requires the implementation of measures that are aligned with HIPAA security and privacy standards. The disaster recovery plan—which comes under the ambit of a contingency plan—is the key element of HIPAA compliance, especially from the availability security principal perspective. This article will review the value and the various aspects of a disaster recovery plan under the HIPAA compliance requirements.[2]

What is a HIPAA disaster recovery plan, and why is it important?

The disaster recovery plan is a detailed strategy, developed and documented, that outlines certain plans of action, processes, and procedures to be followed in case of an unforeseen event causing business disruption. This plan aims to reduce the damage or disruption due to such an event and ensure quick recovery from the incident.

Healthcare organizations hold a huge database of patient information that should be protected at all costs. The organization also needs to ensure that they have a contingency plan in place in case of an event or business disruption resulting in no accessibility of critical information or data.

So, now let's review why a HIPAA disaster recovery plan is crucial.

Protects PHI data

The growing popularity of offering easy and anytime access to patient records through healthcare apps has also resulted in high-level security exposure and threats. Moreover, high reliance on electronic PHI (ePHI) data across departments has also pushed the need for strong security measures. With a disaster recovery plan in place—even in case of an unforeseen event—the contingency plan helps restore lost data and secure it in another safe location. This way, the disaster recovery plan ensures compliance with HIPAA and meets the Security Rule and Privacy Rule.

Prevents downtime

Managing sensitive PHI data can be challenging. Given the complexity of healthcare operations and the huge amount of data that organizations deal with, healthcare organizations need to ensure the security and availability of critical data and applications. A disaster recovery plan ensures the availability of essential data and applications, thereby preventing the high-level downtime caused due to the disruption of operations. The strategy provides the healthcare organization with good control over the use of data, safeguarding the availability of critical applications and data. The strategy further provides peace of mind to the organization regarding securing the data.

Ensuring compliance

Organizations within the healthcare industry are expected to meet the HIPAA rules and ensure compliance. Failing to comply with HIPAA may result in hefty fines and penalties. Establishing and implementing a disaster recovery plan prevents HIPAA Security and Privacy rules violations.