netskope

Top 3 Use Cases for HIPAA Compliance in the Cloud

Introduction

Cloud services allow organizations to increase productivity and reduce costs by making information accessible anytime, anywhere and via any device. For healthcare organizations, that productivity can entail new risks: covered entities are still responsible for securing protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules when they outsource functions like data storage to cloud services.

Cloud access security brokers (CASBs) are an integral part of a Security Service Edge (SSE) solution and enable organizations to extend their information protection policies and programs from on-premises infrastructure and applications to cloud services.

Here are the top three use cases for healthcare organizations wishing to avoid fines and breach notifications for HIPAA violations in the cloud:

- PHI policy enforcement across all cloud services
- Intelligent encryption
- Cloud ransomware protection

1 PHI policy enforcement across all cloud services

In a 2013 breach that resulted in a $2M fine settlement, residents and physicians-in-training had stored patient information in a Google-based cloud system that was not approved for storing such data.

This could have been prevented with a CASB solution that supports a rule to “block uploads of PHI to any cloud service if the service is not sanctioned or the user is not authorized.”

Functional Requirements

- Be aware of context (e.g., activities such as “upload,” “download,” and “share”)
- Correlate users’ identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- See and control usage in both sanctioned and unsanctioned cloud services, including unsanctioned instances of sanctioned cloud services (e.g., personal vs. corporate instances of Office 365)
- Integrate with enterprise directory to enforce policies at a group or organizational unit level (e.g., visiting medical staff, hospital administrators, finance staff)
- Decrypt SSL and decode the unpublished API to understand the transaction

2 Intelligent encryption

For example, apply strong encryption with enterprise key management to cloud content containing PHI. Sounds simple enough, but accurately identifying PHI among millions of records that contain inconsistent data is often not straightforward.

The industry-leading Netskope CASB solution has enabled a number of hospitals to accurately enforce data loss prevention (DLP) policies on content already uploaded to cloud services — or en route to or from cloud services — that contains users' medical record numbers (MRNs), even when those numbers have no identifiers and have no standard format.

Functional Requirements

- Be aware of context (e.g., activities such as "upload")
- See and control usage in both sanctioned and unsanctioned cloud services, including unsanctioned instances of sanctioned cloud services (e.g., personal vs. corporate instances of Box)
- Detect sensitive content in a variety of methods, including via a custom keyword dictionary
- Apply strong encryption to sensitive content with enterprise key management
- Integrate with KMIP-compliant key manager
- Decrypt SSL and decode the unpublished API to understand the transaction

3 Cloud ransomware protection

In 2016, one hospital was locked out of its electronic health records (EHR) system for a week, forcing it to return to pen and paper, until the decision was made to pay a $17,000 Bitcoin ransom. Research suggests that healthcare companies are the primary targets for ransomware attacks, even as new variants of ransomware are designed for faster propagation via cloud file sharing services.

Netskope protects healthcare organizations from ransomware in the cloud with advanced visibility and control. For example, the ability to detect, quarantine, and remediate ransomware being downloaded from unsanctioned cloud services in real time.

Functional Requirements

- Inspect, detect, block, and remediate malware in sanctioned cloud services
- Inspect, detect, block, and remediate malware en route to/from unsanctioned cloud services
- Have visibility over cloud traffic even if it's coming from a sync client, native app, or mobile device
- Decrypt SSL and decode the unpublished API to understand the transaction

Conclusion

When evaluating CASB and SSE solutions for HIPAA compliance in the cloud, be sure to verify the vendor's ability to support these top use cases, including the ability to define and enforce PHI policy across all cloud services, including those known to IT and the unknown "shadow IT" services; the ability to intelligently identify PHI within inconsistently formatted records and apply strong encryption; and the ability to detect, block and remediate ransomware. Look for vendors who can do all this for data en route to or from cloud services as well as data already resident in the cloud.

Netskope is the leader in cloud security for healthcare. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope—security evolved. Want to see Netskope cloud security for healthcare in action? Visit www.netskope.com.

Netskope Active Platform | Security Evolved

For more insights on cloud security for healthcare, please go to:

www.netskope.com/request-demo