Addressing Regulatory Cloud Imperatives: HIPAA-Compliant Cloud DLP with Customer-Managed Keys

Shruti Malik
ITEC5010 – Security & Enterprise Networks
Capella University
September 10, 2025

Introduction

This paper evaluates how a healthcare organization can migrate office productivity and data storage to a public cloud while meeting the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The proposed security control is an inline Cloud Access Security Broker (CASB) with integrated Data Loss Prevention (DLP) and customer-managed encryption keys (CMEK/BYOK) backed by a cloud Key Management Service (KMS) using Hardware Security Modules (HSMs). This control is framed within Zero Trust Architecture (ZTA) principles and mapped to HIPAA technical, administrative, and organizational safeguards.

Risks and Threats of Moving to a Public Cloud

Public cloud adoption introduces a distinct set of risks for protected health information (PHI) and supporting systems:

- Misconfiguration and excessive permissions that expose cloud storage or SaaS data to the public Internet or broad internal audiences.
- Compromised identities (e.g., phishing, password reuse) driving unauthorized access to SaaS platforms and IaaS/PaaS APIs.
- Ransomware and data-extortion campaigns targeting healthcare, disrupting availability and exfiltrating PHI.
- API abuse, OAuth token theft, and supply-chain attacks in SaaS ecosystems (e.g., third-party add-ins).
- Loss of visibility, fragmented logging across SaaS/IaaS services, and difficulties in meeting audit requirements.
- Data residency, cross-border transfer issues, and vendor lock-in complicating incident response and eDiscovery.

These threats are well-documented in sector and industry reports (e.g., HHS HC3 ransomware advisories and the Verizon Data Breach Investigations Report) and are exacerbated by the shared-responsibility model—where cloud providers secure the infrastructure while customers must configure identities, data controls, and logging correctly.

Regulatory Rule: HIPAA Security Rule and Cloud Shared Responsibility

HIPAA's Security Rule requires regulated entities (covered entities and business associates) to implement administrative, physical, and technical safeguards that ensure the confidentiality, integrity, and availability of electronic PHI (ePHI). Under OCR's cloud computing guidance, a cloud service provider (CSP) that creates, receives, maintains, or transmits ePHI is a Business Associate—even for "no-view" services where data is encrypted and the CSP lacks the decryption key—and must sign a Business Associate Agreement (BAA). Organizations must also perform a risk analysis and manage risks appropriate to the cloud service model and SLA terms.

Selected Security Control: Inline CASB with Cloud DLP and Customer-Managed Keys (CMEK)

Control Summary—Deploy an inline CASB (forward proxy or SASE Secure Web Gateway insertion) that inspects, classifies, and enforces policy on outbound and inbound cloud traffic for sanctioned SaaS (e.g., Microsoft 365, Google Workspace) and IaaS/PaaS storage (e.g., AWS S3, Azure Blob). Enable cloud DLP policies tuned to PHI (e.g., ICD-10 codes, MRNs, SSNs) with contextual rules (user role, device posture, location). Enforce encryption at rest with CMEK/BYOK using a KMS backed by HSMs; keys are tenant-owned, with separation of duties and dual control. Integrate IdP/SSO with MFA and conditional access to support Zero Trust and least privilege.

How It Protects Cloud Data—
• Prevents exfiltration: Blocks or quarantines uploads, shares, and email attachments containing PHI to unauthorized destinations; redacts or tokenizes sensitive fields for approved workflows.
• Minimizes blast radius: Applies role- and device-aware policies (e.g., read-only from unmanaged devices, watermarking, session recording) and prevents risky third-party SaaS connections.
• Enforces strong cryptography: Ensures all ePHI is encrypted at rest with customer-controlled keys (CMEK/BYOK) and in transit via TLS; logs all key operations to a SIEM.
• Improves auditability: Centralizes visibility, produces exportable, immutable logs (access, DLP incidents, key events), and supports investigations and compliance audits.

Logical Network Diagram and Control Placement

Figure 1 illustrates a hierarchical design: users authenticate with MFA to the IdP/SSO; traffic to cloud services is steered through a SASE Secure Web Gateway with inline

CASB/DLP. A tokenization service supports de-identification for analytics, while customer-managed keys are hosted in KMS/HSM. Cloud audit logs and DLP/key events flow to the SIEM for monitoring and evidence collection.

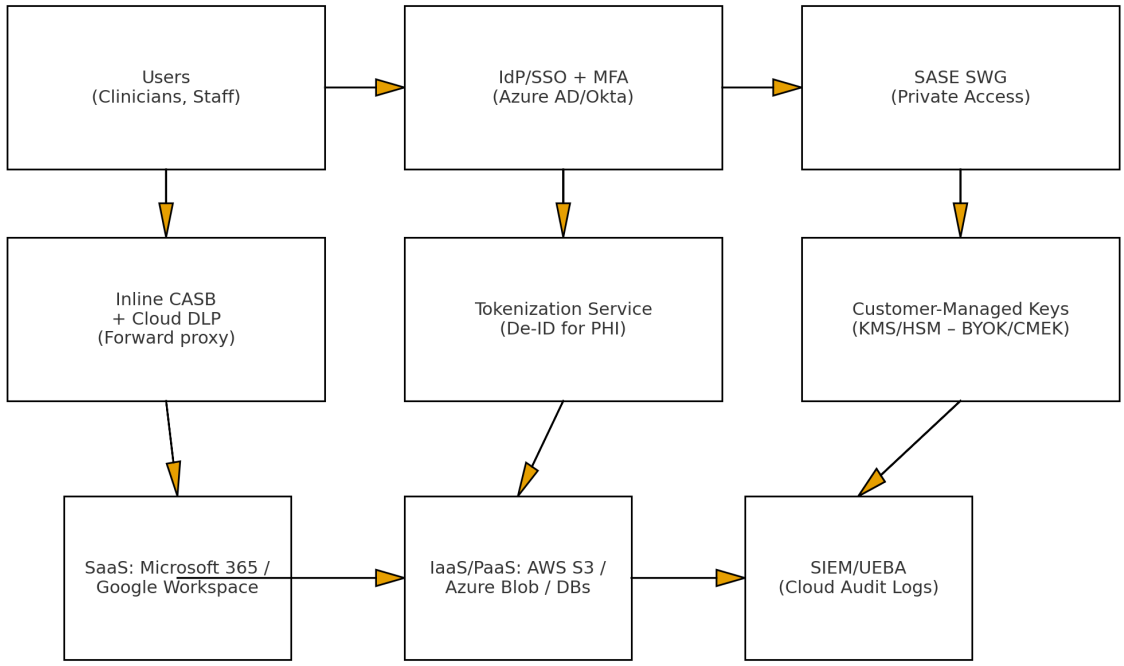

Figure 1. HIPAA-aligned placement of inline CASB/DLP and Customer-Managed Keys (CMEK) in a Zero Trust cloud access design.

How the Control Enables HIPAA Compliance

The control directly supports HIPAA Security Rule implementation specifications and recognized security practices:

• 45 CFR §164.312(a) Access Control & Unique IDs; §164.312(d) Authentication; §164.312(e) Transmission Security—CASB enforces authenticated access via IdP/MFA and ensures TLS for data in motion.

• 45 CFR §164.312(a)(2)(iv) Encryption & Decryption; §164.312(c)(1) Integrity—CMEK/BYOK provides tenant-controlled encryption at rest; hashing/digital signatures preserve integrity where applicable.

• 45 CFR §164.312(b) Audit Controls; 45 CFR §164.308(a)(1)(ii)(D) Information System Activity Review—DLP incidents, access decisions, and key-usage logs create an auditable trail exported to SIEM/UEBA.

• 45 CFR §164.308(a)(4)(ii)(B) Access Authorization; §164.308(a)(3) Workforce

Security—Contextual policies, least-privilege and device-based restrictions reduce unauthorized uses and disclosures.

• Recognized Security Practices (HITECH §13412)—Alignment with NIST SP 800-66r2 (HIPAA implementation), NIST SP 800-207 (Zero Trust), CIS Controls v8.1 (Control 3: Data Protection), and CSA CCM v4 strengthens OCR's consideration of adopted practices over the prior 12 months.

Conclusion

Moving productivity and storage to the public cloud can satisfy HIPAA requirements when paired with the right controls. An inline CASB with DLP and CMEK materially reduces the likelihood and impact of misconfiguration, credential abuse, and exfiltration while improving auditability and incident response. By anchoring the design in Zero Trust, aligning to NIST, CIS, and CSA guidance, and memorializing responsibilities in the BAA and SLAs, the organization maintains confidentiality, integrity, and availability of ePHI in a measurable, auditable manner.

References (APA 7th)

U.S. Department of Health & Human Services, Office for Civil Rights. (2024, December 30). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health & Human Services, Office for Civil Rights. (2022, December 6). Guidance on HIPAA & Cloud Computing. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/

National Institute of Standards and Technology. (2024). NIST SP 800-66r2: Implementing the HIPAA Security Rule. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

National Institute of Standards and Technology. (2020). NIST SP 800-207: Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207

Center for Internet Security. (2024). CIS Critical Security Controls v8.1. https://www.cisecurity.org/controls/v8-1

Cloud Security Alliance. (2025). Cloud Controls Matrix (CCM) v4. https://cloudsecurityalliance.org/research/cloud-controls-matrix

U.S. Department of Health & Human Services, HC3. (2024, April 5). HC3's Top 10 Most Active Ransomware Groups (TLP:CLEAR). https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf

Verizon. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

U.S. Department of Health & Human Services, Office for Civil Rights. (2024, October 24). Security Rule Guidance Material: Recognized Security Practices. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html