SOLUTION BRIEF

Achieving HIPAA compliance

The Health Insurance Portability and Accountability Act, also known as HIPAA, is a set of US standards outlining the protection of sensitive patient data. HIPAA requires that anyone dealing with protected health information (PHI), including electronic protected health information (ePHI), have appropriate security measures in place. Organizations that must comply with HIPAA include covered entities (e.g., healthcare organizations that electronically collect, create, or transmit PHI) and business associates (e.g., organizations working on behalf of a covered entity that encounter PHI). The HIPAA Security Rule Standards and Implementation Specifications consists of four sections meant to identify security safeguards that can help achieve compliance: 1) Physical, 2) Administrative, 3) Technical, and 4) Policies, Procedures, and Documentation Requirements. Adhering to these standards ensures that organizations keep PHI and ePHI private and secure.

Lacework can help with HIPAA compliance by easily providing a comprehensive view of your cloud environment and mapping HIPAA controls to the cloud security controls monitored by Lacework. Lacework reports can be run at any point in time to review compliance against your multicloud and multi-account environment, allowing your compliance team and cloud team to work together to support continued compliance to HIPAA.

Additionally, Lacework reports can be run and reviewed over different time periods, so any compliance drifts can be reviewed and investigated. Lacework also facilitates the auditing process: at any time, you can choose to run a report that shows exactly how your cloud environment implements HIPAA controls, which you can then provide to an auditor. Our platform saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit.

The unique Lacework HIPAA advantage

Lacework acts as a “flight data recorder” for your environment, collecting and organizing relevant data. We enable organizations to easily meet auditors’ evidence gathering requests, drastically reducing the amount of time required for your security or compliance team. In addition, we track this data over time so that you can always go back and review changes to ensure better control of your environment.

Using the Lacework Polygraph® Data Platform

The Lacework Platform contains many features that will help streamline your journey to HIPAA compliance, including:

Asset management

Track your cloud resources with the Lacework resource management function. You can edit the resources summary to show different information, including Resource Name, Account ID, Account Alias, Service, Type, Status, etc. You can also export the resource summary to a CSV file, which you can use as evidence of your organization's cloud asset inventory.

Logging and monitoring

Automated monitoring and reporting throughout the development lifecycle helps ensure that you're compliant from day one. Lacework monitors cloud events, configurations, and behavioral activities, offering you a complete view of your entire cloud ecosystem. The events dashboard gives an overview of all events that have been logged in their environment. Event records include a description of why the event was triggered, which account was responsible, what API was affected, and the source IP address. Lacework also enables you to send high-fidelity contextual alerts to your SIEM solution.

Vulnerability scanning

By managing vulnerabilities and compliance continuously, you can mitigate risk as it is introduced into your cloud infrastructure. Lacework automatically and continuously scans your organization's cloud environment for vulnerabilities, which we communicate via alert channels configured by the admin user. The Lacework Vulnerability Assessment summary shows a list of all identified vulnerabilities and rates them based on criticality. You can then export the report to a CSV file to share with auditors.

Host intrusion detection system (HIDS)

Lacework acts as a host-based intrusion detection system (HIDS) where an agent is loaded into various types of Linux workloads to gain visibility into changes in baseline behaviors. Lacework can also monitor Kubernetes-based workloads as well as files within containers and VMs.

Compliance over time

Lacework allows for tracking of compliance standards over time. A user can run a compliance report at any time to see the compliance status on an hour-by-hour basis. This enables tracking of compliance status to see what has changed and who changed it.

Communication and information

The Lacework compliance dashboard provides an overview of your organization's compliance posture across all your accounts. It also groups the HIPAA technical controls into a readable PDF or CSV format. The report covers areas such as identity and access management, logging and monitoring, networking, and general security. Plus, it displays how your organization's cloud configurations are mapped to specific HIPAA criteria, showing which need to be addressed and fixed. With our one-click reporting, you can stop aggregating reports from multiple systems, and start responding to auditors instantly.

Mapping required security controls

HIPAA control numbers	Lacework Polygraph Data Platform
Access Control §164.312(A)(1)	Included
Audit Controls §164.312(B)	Included
Person or Entity Authentication §164.312(D)	Included
Transmission Security §164.312(E)(1)	Included

Ready to chat?

Request a demo