Likewise®

Fact Sheet

HIPAA Compliance For File Servers and Storage Systems

This fact sheet describes Likewise's security controls for electronic protected health information stored on file servers and NAS systems. Specifically, the fact sheet details how Likewise addresses the Administrative Safeguards and the Technical Safeguards sections of the HIPAA Security Rule.

The fact sheet also discusses how Likewise's architecture provides the foundation and the functionality to perform continuous monitoring of unstructured health data to address emerging information security guidelines from the National Institute of Standards and Technology (NIST).

HIPAA mandates that you protect information and information systems to provide confidentiality, integrity, and availability. To do so, you must implement security controls in accordance with NIST Special Publication 800-53.

Likewise software helps ensure the confidentiality, availability, and integrity of health information in storage systems by implementing security controls that cost-effectively protect against unauthorized access, use, disclosure, disruption, modification, or destruction. In particular, as described below, Likewise implements many of the security controls for access control, system monitoring, reporting, and audit and accountability.

Mapping Security Controls from NIST SP 800-53 to Likewise Capabilities

The following sections detail the technical and administrative security controls that Likewise can put in place to help ensure the security of information and systems.

Likewise makes two software products: The Likewise Storage Services platform and the Likewise Data Analytics and Governance application.

In general, the Likewise Storage Services platform provides authentication and access control for file servers running on Linux and Unix computers by using Microsoft Active Directory or another user directory.

The Likewise Data Analytics and Governance application collects, aggregates, stores, analyzes, audits, monitors, and reports on events that take place on file servers and storage systems, including NetApp, HP servers, and EMC NAS devices.

Technical Safeguards

This section maps the Technical Safeguards sections of the HIPAA Security Rule to the recommended security controls defined in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, and then describes Likewise's capabilities in establishing each security control.

The mapping of the HIPAA Technical Safeguards to the security controls in 800-53 is based on the mappings in NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Security controls that are not applicable are not discussed.

HIPAA 164.312(a)(1) Access Control

Standard: "Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

NIST SP 800-53 Security Control Mapping: AC-1, AC-3, AC-5, AC-6.

Likewise Support: *AC-3 Access Enforcement*: On Unix and Linux file servers, Likewise Storage Service enforces access controls through Active Directory or another access control system, such as LDAP.

AC-5 Separation of Duties: By connecting Linux and Unix file servers to Microsoft Active Directory or another directory service, Likewise Storage Services can implement or help implement separation of duties for users based on the settings in the directory service.

AC-6 Least Privilege: Likewise ports the access rights, including those based on least privilege, from Active Directory to Linux and Unix file servers running the Likewise Storage Services platform.

HIPAA 164.312(a)(2)(i) Unique User Identification

Implementation Specification: "Assign a unique name and/or number for identifying and tracking user identity."

NIST SP 800-53 Security Control Mapping: AC-2, AC-3, IA-2, IA-3, IA-4.

Likewise Support: *AC-2 Account Management*: Likewise helps foster centralized account management by connecting Linux and Unix file servers to Microsoft Active Directory or another account management system and then extending the capabilities of that account management system to the file servers.

AC-3 Access Enforcement: On Linux and Unix file servers, Likewise enforces access controls through Active Directory or another access control system, such as NIS.

IA-2 Identification and Authentication: Likewise Storage Services performs identification and authentication of organizational users on Linux and Unix file servers by using Active Directory or another user directory, such as LDAP.

IA-4 Identifier Management: Likewise enables organizations to use the unique identifiers selected for individuals in an identity management system, such as Active Directory, on Linux file servers.

HIPAA 164.312(b) Audit Controls

Standard: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

NIST SP 800-53 Security Control Mapping: AU-1, AU-2, AU-3, AU-4, AU-6, AU-7.

Likewise Support: *AU-2 Auditable Events*: Likewise collects and stores the events that take place on file servers and NAS systems. You can choose which events to record as auditable events. Likewise collects the following types of events and ties them to the identity of users without impairing the system's performance: authentication requests and access attempts; attempts to view, modify, add, or delete directories and files; and attempts to modify the security descriptors of files or directories.

AU-3 Content of Audit Records: Likewise collects and stores audit records that show the type of each event and its data, time, source, location, IP address, outcome, and other data. Likewise also captures the identity of the user or aon associated with the event.

AU-4 Audit Storage Capacity: The Likewise application allocates storage capacity for audit records by using a uniquely scalable and high-performance NoSQL database that not only reduces the likelihood of its capacity being exceeded but also scales cost-effectively to handle millions of events.

AU-6 Audit Review, Analysis, and Reporting: Likewise analyzes audit records from storage systems. When it finds indications of inappropriate or unusual activity, it sends a security alert to designated sources. You can adjust Likewise's review and analysis thresholds to meet changing levels of risk. There is support for several control enhancements: Likewise acts as a security event and information management system to correlate and analyze audit records from different repositories, providing organization-wide situational awareness.

AU-7 Audit Reduction and Report Generation: Likewise supports near real-time audit reviews, analysis, and reporting as well as investigations of security incidents without altering the original audit records. In addition, Likewise can automatically process audit records for events of interest based on criteria that you select and display the records on a dashboard.

HIPAA 164.312(d) Person or Entity Authentication

Standard: "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

NIST SP 800-53 Security Control Mapping: IA-2, IA-3, IA-4.

Likewise Support: *IA-2 Identification and Authentication*: Likewise Storage Services performs identification and authentication of organizational users on Linux and Unix file servers by using Active Directory or another user directory.

IA-4 Identifier Management: Likewise enables organizations to use the unique identifiers selected for individuals in an identity management system, such as Active Directory, on Linux file servers.

Administrative Safeguards

This section maps the Administrative Safeguards sections of the HIPAA Security Rule to the recommended security controls defined in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, and then describes Likewise's capabilities in establishing each security control.

The mapping of the Technical Safeguards to the security controls in 800-53 is based on the mappings in NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Security controls that are not applicable are not discussed.

HIPAA 164.308(a)(1)(ii)(D) Information System Activity Review (R)

Implementation Specification: "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

NIST SP 800-53 Security Control Mapping: AU-6, AU-7, CA-7, IR-5, IR-6, SI-4.

Likewise Support: *AU-6 Audit Review, Analysis, and Reporting:* Likewise analyzes audit records from storage systems. When it finds indications of inappropriate or unusual activity, it sends a security alert to designated sources. You can adjust Likewise's review and analysis thresholds to meet changing levels of risk. There is support for several control enhancements: Likewise acts as a security event and information management system to correlate and analyze audit records from different repositories, providing organization-wide situational awareness.

AU-7 Audit Reduction and Report Generation: Likewise supports near real-time audit reviews, analysis, and reporting as well as investigations of security incidents without altering the original audit records. In addition, Likewise can automatically process audit records for events of interest based on criteria that you select and display them on a dashboard.

IR-5 Incident Monitoring: Likewise's monitoring system helps you track security incidents on file servers and storage systems by displaying the incidents on a dashboard and by recording them in its database. Likewise can maintain records about each incident, the status of the incident, and other information for forensics, forecasting, and trend analysis.

SI-4 Information System Monitoring: Likewise helps your organization monitor events on file servers, NAS systems, and other data storage systems. Likewise tracks specific types of transactions and displays them on a dashboard for situational awareness. For SI-4, Likewise supports several control enhancements, such as providing near real-time alerts when indications of compromise or potential compromise occur and notifying incident response personnel of suspicious events.

HIPAA 164.308(a)(3)(i) Workforce Security

Standard: "Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information."

NIST SP 800-53 Security Control Mapping: AC-1, AC-5, AC-6.

Likewise Support: *AC-5 Separation of Duties:* By connecting Linux and Unix file servers to Microsoft Active Directory or another directory service, the Likewise Storage Services platform can implement or help implement separation of duties for users based on the settings in the directory service.

AC-6 Least Privilege: Likewise ports the access rights, including those based on least privilege, from Active Directory or another directory service to Linux and Unix file servers.

HIPAA 164.308(a)(4)(ii)(B) Access Authorization (A)

Implementation Specification: "Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

NIST SP 800-53 Security Control Mapping: AC-1, AC-2, AC-3, AC-4, AC-13, PS-6, PS-7.

Likewise Support: *AC-2 Account Management*: Likewise helps foster centralized account management by connecting Linux and Unix file servers to Microsoft Active Directory or another account management system.

AC-3 Access Enforcement: Likewise enforces access controls through Active Directory or another access control system, such as NIS.

HIPAA 164.308(a)(4)(ii)(C) Access Establishment and Modification (A)

Implementation Specification: "Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

NIST SP 800-53 Security Control Mapping: AC-1, AC-2, AC-3.

Likewise Support: *AC-2 Account Management:* Likewise helps foster centralized account management by connecting Linux and Unix file servers to Microsoft Active Directory or another account management system.

AC-3 Access Enforcement: Likewise enforces access controls through Active Directory or another access control system, such as NIS.

HIPAA 164.308(a)(5)(ii)(C) Log-in Monitoring (A)

Implementation Specification: "Procedures for monitoring log-in attempts and reporting discrepancies."

NIST SP 800-53 Security Control Mapping: AC-2, AC-13, AU-2, AU-6.

Likewise Support: *AC-2 Account Management*: Likewise helps foster centralized account management by connecting Linux and Unix file servers to Microsoft Active Directory or another account management system.

AU-2 Auditable Events: Likewise collects and stores the events that take place on file servers and NAS systems. You can choose which events to record as auditable events. Likewise collects the following types of events and ties them to the identity of users without impairing the system's performance: authentication requests and access attempts; attempts to view, modify, add, or delete directories and files; and attempts to modify the security descriptors of files or directories.

AU-6 Audit Review, Analysis, and Reporting: Likewise analyzes audit records from storage systems. When it finds indications of inappropriate or unusual activity, it sends a security alert to designated sources. You can adjust Likewise's review and analysis thresholds to meet changing levels of risk. There is support for several control enhancements: Likewise acts as a security event and information management system to correlate and analyze audit records from different repositories, providing organization-wide situational awareness.

HIPAA 164.308(a)(6)(ii) Response and Reporting (R)

Implementation Specification: "Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

NIST SP 800-53 Security Control Mapping: IR-4, IR-5, IR-6, IR-7.

Likewise Support: *IR-5 Incident Monitoring*: Likewise's monitoring system helps you track security incidents on file servers and storage systems by displaying the incidents on a dashboard and by recording them in its database. Likewise can maintain records about each incident, the status of the incident, and other information for forensics, forecasting, and trend analysis.

Architecture for Continuous Monitoring

The architecture of Likewise Data Analytics and Governance can take you beyond fulfilling the minimum requirements of HIPAA and into the realm of maintaining situational awareness through continuous monitoring. The Likewise application, for example, collects, correlates, and analyzes all security-related events on file servers and network attached storage, giving you visibility into your storage assets and the users who access them.

The tremendous amount of data from continuous monitoring requires a solution that can scale. Likewise's commercially hardened SQL and NoSQL infrastructure with polyglot persistence can scale beyond a departmental deployment to support storage arrays with hundreds of millions of file objects and high workloads. It can pull data from a variety of information sources through a RESTful interface. It provides reports that range from high-level, aggregate metrics to system-level metrics. With a built-in dashboard, it acts as security information and event management (SIEM) tool for storage systems.

To take you into the future of information security, the architecture and functionality of the application helps you establish a continuous monitoring program as defined in *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST Special Publication 800-137).

Next Steps

For more information on Likewise, visit the web site at **www.likewise.com**. To contact the sales team, call (800) 378-1330 or email **info@likewise.com**.

References

- NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

15395 SE 30th Pl, Suite 140, Bellevue, WA, 98007. (800) 378-1330