Lepide

Mapping the Lepide Data Security Platform to **HIPAA Security Controls**

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was put in place in 1996 to continuously develop regulations protecting the privacy and security of electronic protected health information, or ePHI as it is commonly known.

It is predominantly broken down into two parts, the HIPAA privacy rule, and the HIPAA security rule.

The privacy rule establishes national standards for the protection of certain health information whereas the security rule enforces a set of security standards for protecting health information that is stored or transferred in electronic form.

The rule applies to organizations that are referred to as covered entities, covered entities include health plans, clearinghouses, and a myriad of healthcare providers such as doctors, nursing homes, dentists, and psychologists to name a few.

The rule was developed by the US department of health and services, within the HHS, the office for civil rights (OCR) has the responsibility for enforcing the privacy and security rules and if violated, can (and quite often will) result in noncompliance penalties and fines imposed on the violating organization.

Requirements Breakdown

The HIPAA security rule states that covered entities should:

1. Ensure the confidentiality, integrity, and availability of all PHI they create, receive, store and transfer
2. Identify and protect against threats to the security and integrity of PHI
3. Protect against prohibited use or disclosures of PHI
4. Ensure all employees and business associates are trained when handling or interacting with PHI

Some aspects that the covered entity is required to consider when deciding the security measures to use are:

1. The size, complexity, and capability of the organization
2. The complete IT infrastructure including all hardware and software
3. The cost to implement the appropriate security measures
4. The likelihood and the possible impact of the potential risk to protected health information

Mapping Lepide to HIPAA Security Controls

Key Activity	HIPAA Specific Control Area	Technology Alignment
Risk Analysis and Management	1) §164.308(a)(1)(ii)(A)- **Security Management Process- Risk analysis** §164.308(a)(1)(ii)(A) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. 2) §164.308(a)(1)(ii)(B)- **Security Management Process**- Risk management- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Human Resources Security	1) §164.308(a)(1)(ii)(C)-**Security Management Process** - **Sanction policy-** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. 2) §164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics)
Isolate Healthcare Clearinghouse Functions	§164.308(a)(4)(ii)(A): **Information Access Management** - If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics)
Incident Response	§164.308(a)(6): **Security Incident Procedures (§164.308(a)(6) (ii))** - 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.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Key Activity	HIPAA Specific Control Area	Technology Alignment
Access Control	§164.312(a)(1) **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).	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics)
Logging, Monitoring and Alerting	§164.312(b) **Audit Controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Information Integrity	1) §164.312(c)(1) **Integrity -** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. 2) §164.312(c)(2) - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Lepide Data Security Platform Core Capabilities

Lepide Identify

(Data Discovery and Classification)

- Discover and classify data in real-time.
- Tag data.
- Data valuation.
- Identify data most at risk.

Lepide Trust

(Access Governance)

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Change permissions.

Lepide Insight

(User and Entity Behavior Analytics)

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

Lepide Detect

(Threat Detection and Response)

- Detect threats in real-time.
- Baseline/profile employee behaviour.
- Identify anomalous employee behaviour.
- Alert and respond to threats in real-time.

Meet HIPAA Compliance with Lepide

Prepare your organization for your next HIPAA audit with Lepide. Lepide provides a complete HIPAA compliance audit software, providing numerous pre-defined HIPAA audit reports to help your organization avoid non-compliance fines.

Secure Patient Data

Ensure users aren't accessing patient data unless they require that access to perform their job role.

Monitor Access to HIPAA Data

Monitor and alert on all user behavior relating to data that falls under HIPAA compliance regulations.

Pre-Set HIPAA Reports

Numerous pre-defined reports tailored to meet some of the more stringent auditing aspects of HIPAA compliance.

Start a free trial

Get a demo

Get a free risk assessment