

A magnifying glass with a black frame is positioned over a white document. The document has the words "HIPAA REQUIREMENTS" printed in a black, serif, all-caps font. The magnifying glass is centered over the text, making it the focal point of the image. In the background, a wooden desk, a red pen, and a black paperclip are visible but out of focus.

# HIPAA REQUIREMENTS



**Lockpath**

A NAVEX Global® Company

**HIPAA audits, compliance  
and risk management  
with Lockpath®**

# HIPAA audits call for an integrated risk management program powered by a GRC platform.

HIPAA Phase 2 audits are well underway. If your healthcare organization receives a desk audit notification letter, you have ten days to respond. Will you be ready if that letter comes?

What if you had a streamlined process for audits, compliance, and risk management, so your healthcare organization didn't have to stress over HIPAA audits?

**Audit-ready with Lockpath**

Many healthcare organizations depend on the Lockpath Platform.

It empowers them to comply with healthcare regulations, conduct assessments that assign risk levels to business associates, manages cybersecurity feeds and provides robust reporting for the CIO and other executives. Above all, Lockpath keeps you audit-ready with up-to-date, accessible, and presentable documentation.

**HIPAA compliance**

If your organization stores or has access to electronic Protected

Health Information (ePHI), you likely have a strong awareness of HIPAA compliance and the hazards of non-compliance.

HIPAA compliance requirements include five rules (Security, Privacy, Breach Notification, Omnibus, Enforcement) and three safeguards (Technical, Physical, Administrative). Each rule and safeguard has its own set of requirements.

Lockpath brings a standardized approach to HIPAA compliance. Some compliance activities can even be set up for automation.

The platform's central repository enables multiple departments to document and conduct compliance activities to meet HIPAA requirements. Everything needed, from controls and policies to requirements and mandates, is linked and made accessible in Lockpath with user access limited to pre-determined roles.

**Conducting risk assessments**

The Office for Civil Rights (OCR)

is responsible for enforcing HIPAA's privacy and security rules. A focus area for the OCR in Phase 2 is ensuring a healthcare organization's business associate risk assessments are accurate, complete and up-to-date.

Lockpath facilitates managing hundreds of assessments and incorporates the OCR's self-risk assessment tools. You can easily create, issue, score and manage business associate assessments and questionnaires. You can save time by using pre-populated assessments and automatic scoring.

With data collected and centrally located in Lockpath, you can perform risk analyses, which can lead to uncovering gaps like an existing vulnerability, so risk and compliance teams know where to direct their attention.

**Preparedness for Phase 2 and beyond**

It's too late to prepare for an OCR audit when you've received the notification. The time to act

HIPAA Compliance Needs	Policy/ Compliance	Risk Mgmt	Third Party	Incident	InfoSec	Audit	Reporting	Assessments
Privacy Rule	✓	✓	✓	✓	✓	✓	✓	✓
Security Rule	✓	✓	✓	✓	✓	✓	✓	✓
Technical Safeguards	✓	✓	✓	✓	✓	✓	✓	✓
Physical Safeguards	✓	✓	✓	✓	✓	✓	✓	✓
Administrative Safeguards	✓	✓	✓	✓	✓	✓	✓	✓
Breach Notification Rule	✓	✓	✓	✓	✓	✓	✓	✓
Omnibus Rule	✓	✓	✓	✓	✓	✓	✓	✓
Enforcement Rule	✓	✓	✓	✓	✓	✓	✓	✓

The Lockpath Platform can help your healthcare organization manage compliance and associated risk management activities with HIPAA rules and safeguards down to their legal citations.

is now. The Lockpath Platform can help your healthcare organization address the three focus areas: audit, compliance and risk management.

The platform keeps you audit-ready, streamlines compliance with HIPAA requirements, and

makes it easier to conduct risk assessments. Not only does Lockpath address these focus areas, it's instrumental in managing other healthcare regulations and requirements associated with protecting patient data, cybersecurity and other compliance requirements.

To learn more about the Lockpath Platform for HIPAA compliance, risk management, and information security, contact us at [info@Lockpath.com](mailto:info@Lockpath.com).

**About NAVEX Global**

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Trusted by more than 14,500 customers, our solutions help organizations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. For more information, visit [www.navexglobal.com](http://www.navexglobal.com).



## Cybercriminals target ePHI. Focus on information security.

Cybercriminals target electronic protected health information (ePHI) because it's highly profitable on the black market. In fact, the FBI issued a warning to healthcare organizations using File Transfer Protocol (FTP) servers as hackers were using FTP to access stored ePHI. Managing information security is a major function in the Lockpath Platform. From connectors to vulnerability scanners to managing incidents and integrating risk management activities across the organization, Lockpath helps prevent cybercrimes and is instrumental in managing recovery efforts when they occur.