www.nightfall.ai

Nightfall™

Guide to HIPAA Compliance on Slack

How to ensure that covered entities set up and maintain their Slack Workspaces in a HIPAA compliant way.

About Nightfall AI

- We are an official Slack partner for Data loss prevention (DLP)
- We work with a variety of HIPAA compliant organizations to secure their Slack instances
- This webinar is designed to give a general overview of standards and best practices, but for detailed information specific to your Slack use case talk to Slack directly

Nightfall™

nightfall.ai/integrations/slack

How does Slack provide HIPAA compliance?

Slack is not HIPAA compliant out of the box.

Specific **standards and controls must be in place** within Slack to ensure the satisfaction of HIPAA requirements.

Before adopting Slack, covered entities need to understand their requirements as well as their intended use case for Slack. This analysis helps organizations determine if they can maintain HIPAA compliance on Slack.

Nightfall™

nightfall.ai/integrations/slack

What requirements must be satisfied for HIPAA Compliance on Slack?

- Appropriate Slack use case
- Slack's HIPAA maintenance requirements
- Suggested Slack hygiene/best practices (**recommended**)
- HIPAA Security Rule considerations

Nightfall™

nightfall.ai/integrations/slack

Examples of HIPAA compliant Slack use cases

Slack is meant to streamline collaboration within healthcare organizations and is not sanctioned for communications between patients and care providers.

Examples:

- Conveniently triage outpatient care with Slack
- Improve productivity around diagnostics and procedures w/ an integrated electronic medical records system
- Real time patient care updates for practitioners

1. “How health-care teams can maintain HIPAA compliance within Slack” - Slack Blog

Nightfall™

nightfall.ai/integrations/slack

Slack's requirements for maintaining HIPAA compliance

- Organization **must be on a Slack Enterprise account**
- Organization **must execute a Business Associate Agreement with Slack**
- **Cannot use Slack for patient communications** as it's not designed to communicate with patients and families
- No PHI in "**prohibited fields**" (file names, user profile data, custom profile fields, custom emojis, custom statuses, workspace and organization names, EMM)

2. "HIPAA-Compliant Collaboration with Slack" - Slack Documentation

Nightfall™

nightfall.ai/integrations/slack

Slack's requirements for maintaining HIPAA compliance (continued)

- PHI can **only be shared in private channels** where only need to know members have access to it
- The **Slack email ingestion tool**, which converts emails to Slack messages, **needs to be disabled** from the admin console
- In-field clinicians **cannot connect over patient Wi-Fi**

2. "HIPAA-Compliant Collaboration with Slack" - Slack Documentation

Nightfall™

nightfall.ai/integrations/slack

Additional details

- According to Slack: **“Slack does not maintain the designated record set and should not be the system of record for your health information.”**
- Your organization is responsible for using Slack APIs to implement security tools and processes for monitoring your members’ use of Slack and securing your workspace.
  Examples of these tools include:
  - Single Sign On (SSO)
  - Backup/Archival
  - Data loss prevention (DLP)

2. “HIPAA-Compliant Collaboration with Slack” - Slack Documentation
3. “Slack and HIPAA” - Slack Help Center Extras

Nightfall™

nightfall.ai/integrations/slack

Recommended Slack hygiene

- Enforce a **consistent channel creation process** that complements business objectives and security policies

- Streamline Slack security with automated features like **message and file retention time limits** that map to your risk management & compliance strategies

- **Identify engaged stakeholders** who will serve as Slack admins and aid employee education

4. “4 Best Practices for Healthcare teams using Slack” - Nightfall AI

Nightfall™

nightfall.ai/integrations/slack

HIPAA Security Rule considerations

The HIPAA Security Rule provides a number of guidelines that are relevant to organizations on Slack, including:

- Identifying and protecting against reasonably anticipated threats to the security or integrity of the information
- Protecting against reasonably anticipated, impermissible uses, or disclosures
- Ensuring compliance of policies by workforce
- Evaluating the likelihood and impact of potential risks to e-PHI
- Implementing appropriate security measures to address the risks identified in the risk analysis

5. “Summary of the HIPAA Security Rule” - HHS.gov Health Information Privacy

Compliance with the HIPAA Security Rule

In addition to following Slack's rules for maintaining HIPAA compliance, organizations will need to ensure they have security tools like **Data Loss Prevention (DLP)** in their workspaces because **Slack relies on third-party vendors** to provide the controls necessary to satisfy HIPAA Security Rule guidelines.

Nightfall™

nightfall.ai/integrations/slack

What is Data Loss Prevention (DLP)?

DLP ensures confidential or sensitive information (like patient names and addresses) isn't shared outside of Slack by scanning for content within messages and files that break predefined policies.

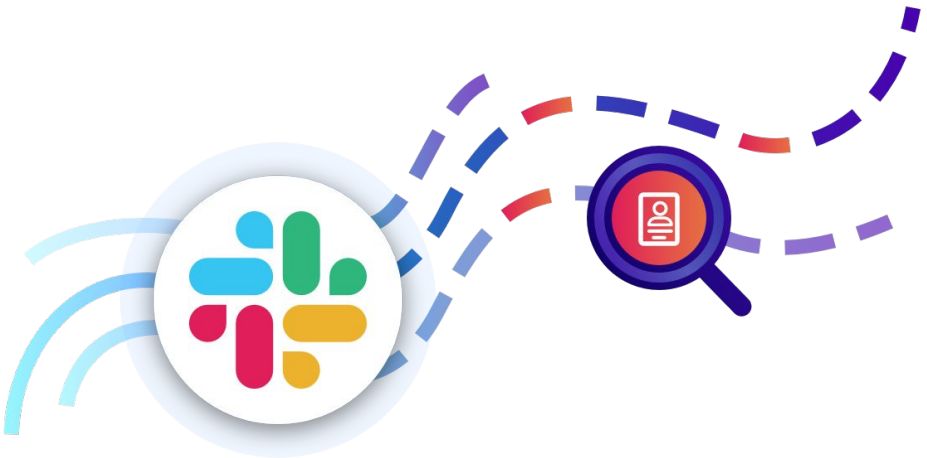
Nightfall™

nightfall.ai/integrations/slack

How does Slack Benefit from DLP?

Collaborative SaaS applications like Slack create environments where data policy and security best practices are difficult to maintain or enforce without an excessive time or resource commitment.

Data loss prevention helps provides companies with a feasible alternative to address this problem.



Nightfall™

nightfall.ai/integrations/slack

What is the Nightfall DLP platform?

- Nightfall is a platform to discover, classify, and protect sensitive data across cloud SaaS & data infrastructure via machine learning.
- Nightfall's Slack bot helps you instantly add DLP functionality to Slack.
- The bot detects sensitive data in files & messages in real-time. Get alerted & take remediative action directly within Slack.
- Nightfall directly supports compliance efforts HIPAA and many other industry regulations.

Nightfall™

nightfall.ai/integrations/slack

How does Nightfall work?

Discover: Continuously monitor sensitive data that is flowing into and out of files & messages in Slack.

Classify: Machine learning classifies your sensitive data & PII automatically, without prior tuning or tagging, so nothing gets missed.

Protect: Setup automated DLP workflows for quarantines, deletions, alerts, coaching, and more - saving you time and keeping your business safe.

Nightfall™

nightfall.ai/integrations/slack

How does Nightfall make Slack HIPAA compliant?

Nightfall allows healthcare organizations to:

- Monitor communication channels like the ones in Slack for PHI
- Place controls to prohibit the sharing of PHI over inappropriate channels
- Implement messaging that educates users about the appropriate contexts for sharing PHI
- Assess PHI risk with detailed analytics of incidents that break policies

Nightfall™

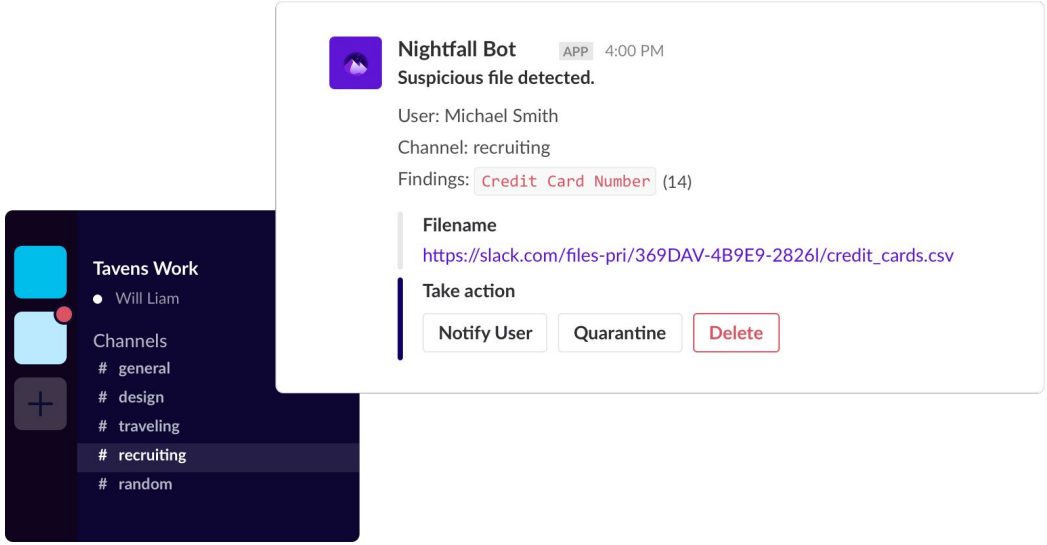
nightfall.ai/integrations/slack

How do I implement Nightfall on Slack?

Nightfall's Slack bot can be added in seconds to your Slack account.

No additional set up, tuning, or installed agents are required.

Request a free trial with us.



Nightfall™

nightfall.ai/integrations/slack

What does Nightfall detect?

Nightfall comes with 100+ detectors out of the box, with the ability to add in custom detectors, rules, keywords, and regexes as well.

Standard PII: Age, Credit Card Number, Email, Ethnic Group, Name, Location, Phone Number

Finance: IBAN, SWIFT, CUSIP, Routing Numbers

Network: IP Address, Hardware ID, MAC Address

IDs: Driver's License Number, Taxpayer ID, Passport Number, Social Security Number, Vehicle ID

Health: ICD, FDA, DEA, NPI, DOB

Crypto: Bitcoin, Ethereum, Litecoin Addresses & Private Keys

Custom: API Keys, your application UUIDs, and much more.

Nightfall™

nightfall.ai/integrations/slack

Does Nightfall scan files too?

Yes Nightfall scans all files & messages. 100+ file types supported (e.g. xls/xlsx, doc/docx, csv, plain text, ppt/pptx, PDF, HTML, etc.).

Nightfall also integrates with many SaaS, data infrastructure, and security products like your SIEM.

Nightfall™

nightfall.ai/integrations/slack

How secure is Nightfall?

- **Does not store or track sensitive findings,** only non-identifying metadata is gathered to improve accuracy.
- TLS 1.2+ in motion and AES 256 at rest encryption.
- Fully hosted on AWS and GCP.

Nightfall™

nightfall.ai/integrations/slack

Case Study: Springbuk

Chris Morrison, Security Coordinator

Industry: SaaS, Healthcare

Employees: 115

Use Cases: HIPAA compliance, DLP, policy enforcement

“Working with Nightfall gives our customers confidence that we take data protection very seriously.”

Nightfall™

nightfall.ai/integrations/slack

Case Study: Galileo Health

galileo

Michael Supon, Head of Security and Compliance

Industry: Healthcare

Employees: 55

Use Cases: HIPAA compliance, DLP, credentials/secrets detection

“Nightfall’s ease of setup and accuracy of identified data are both on point. Nightfall has eased our collective mind.”

Nightfall™

nightfall.ai/integrations/slack

How do I get started?

To get started with Nightfall, request a demo or free trial or email us at sales@nightfall.ai with any questions.

Request a demo or free trial

Not ready yet? Learn more at www.nightfall.ai or contact us at sales@nightfall.ai.

Disclaimer: While we have made every attempt to ensure that the information contained in this presentation is accurate to our best efforts, Shoreline Labs, Inc., is not responsible for any errors or omissions, or for any result obtained from the use of this information. This presentation is based on a specific point in time, and is no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information. Nothing in this presentation should be used as a substitute for the independent investigations and the sound technical and business judgment of your legal and compliance professionals. We do not accept any liability if this presentation is used for an alternative purpose from which it is intended, nor to any third party for any purpose. In no event will Shoreline Labs, Inc., its employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on this presentation or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Nightfall™

nightfall.ai/integrations/slack