Compliance Series

Health Insurance Portability and Accountability Act (HIPAA)

Using the Netskope Platform to Assist with HIPAA Compliance

TABLE OF CONTENTS

INTRODUCTION

When the Health Insurance Portability and Accountability Act (HIPAA) was first passed, it contained no provisions relating to data privacy or data security. Instead, Congress delegated rulemaking authority to the Department of Health and Human Services (HHS).

HHS subsequently prescribed a series of standards and accompanying implementation specifications that have come to be known simply as the Security Rule (45 CFR 164.302-318), the Breach Notification Rule (45 CFR 164.400-414), and the Privacy Rule (45 CFR 164.500-534).

The Privacy Rule prescribes why, when, and to whom protected health information (PHI) can be disclosed, as well as data subjects' right to notice and opportunity to give or withhold consent to the collection or disclosure of their PHI.

Protected Health Information (PHI) includes any identifiable health-related information.
Examples of PHI are:

- Personal Details
- Medical Information
- Biometric Identifiers
- Financial Information
- Dates (Birth/Death etc)
- Other Identifiers (Account/Certificate/License etc)

The Security Rule specifies how data subjects' privacy should be protected. It imposes requirements - such as workforce training, physical access controls, and disaster recovery preparedness - that aim to safeguard PHI from all manner of threats, whether malicious, inadvertent, or natural.

Finally, the Breach Notification Rule promotes transparency and accountability in the handling of PHI, by requiring custodians of PHI to communicate the nature and severity of data breaches to affected data subjects, the general public, and the Secretary of HHS.

HOW TO USE THIS GUIDE

The Netskope platform consists of a suite of tools integrated into a unified Secure Access Service Edge architecture encompassing all the standards prescribed by the Security Rule. The tools can also be used to raise alerts and automate workflows to facilitate compliance with the Breach Notification Rule.

The tables below break down the Security Rule and Breach Notification Rule by Standard and accompanying Implementations. Each Implementation is mapped to an appropriate tool or tools, with a description of how the Netskope platform assists with the organization's compliance needs.

The Standards of the Security Rule fall within three broad categories: administrative safeguards, physical safeguards, and technical safeguards.

Note the following acronyms and/or aliases for the Netskope products:

Industry terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next-Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent AccessI
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

SECTION 164.306 SECURITY STANDARDS: GENERAL RULES

Subsection	Requirements(s)	Netskope Response	Products
164.306(a)	1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. 2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. 3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. 4. Ensure compliance with this subpart by its workforce.	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Additionally, Netskope can assist communication and track acknowledgement of policies through pop-up banners and coaching pages across its products, notifying employees of potential policy infringements, requesting a justification for risky actions, suggesting alternatives, or referring users for further training on organizational or regulatory requirements.	• All products
164.306(b)	1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. 2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors: i. The size, complexity, and capabilities of the covered entity or business associate. ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. iii. The costs of security measures iv. The probability and criticality of potential risks to electronic protected health information.	Netksope assists organizations in implementing a network security architecture that's aligned with industryrecognized cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties. Furthermore Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SDWAN, traffic is steered through Netskope's global New Edge network, allowing high availablility connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on contextspecific criteria such as user, location, device, app instance, and more.	• All products • SD-WAN

Subsection	Requirements(s)	Netskope Response	Products
164.306(c)	1. A covered entity or business associate must comply with the applicable standards as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information.	Netksope assists organizations in implementing a network security architecture that's aligned with industry recognized cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties. Furthermore Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SDWAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on contextspecific criteria such as user, location, device, app instance, and more.	• All products • SD-WAN
164.306(d)	1. (Instructions regarding the interpretation and application of implementation specifications.)	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Additionally, Netskope can assist communication and track acknowledgement of policies through pop-up banners and coaching pages across its products, notifying employees of potential policy infringements, requesting a justification for risky actions, suggesting alternatives, or referring users for further training on organizational or regulatory requirements. Netksope assists organizations in implementing a network security architecture that's aligned with industry recognized cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties. Furthermore Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SDWAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context specific criteria such as user, location, device, app instance, and more..	• All products • SD-WAN

Subsection	Requirements(s)	Netskope Response	Products
164.306(e)	1. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).	A Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM also routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management (SSPM) continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations. SSPM alerts provide step-by-step instructions for remediation, and SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted.	• All products • Advanced • Analytics • CTO • SSPM • CSPM

SECTION 164.308 ADMINISTRATIVE SAFEGUARDS

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(1)(i)	1. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Additionally, Netskope can assist communication and track acknowledgement of policies through pop-up banners and coaching pages across its products, notifying employees of potential policy infringements, requesting a justification for risky actions, suggesting alternatives, or referring users for further training on organizational or regulatory requirements. Netksope assists organizations in implementing a networksecurity architecture that’s aligned with industry-recognized cybersecurity and data privacy best practices. This includes a “defense-in-depth” strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties..	• All products

Subsection	Requirements(s)	Netskope Response	Products
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. B. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. C. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. D. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Remote Browser Isolation is a built-in feature of Netskope's NG-SWG that isolates risky and uncharacterized web sites in a secure, cloud-based container or "sandbox," preventing unauthorized software execution. Any malware is executed in the container and cannot infect the organization's network. Netskope's Standard Threat Protection protects against known malware, uses machine learning analysis to detect new malware, and provides real-time phishing detection, corroborative sandboxing, and web filtering. Netskope Threat Protection integrates with threat intelligence feeds from Netskope's Cloud Threat Exchange, and with other Netskope Intelligent Security Service Edge tools including Remote Browser Isolation, Cloud Firewall, and User Entity and Behavior Analytics to create a layered, defense-indepth security solution. Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's context-aware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions.	• RBI • Threat Protection • Advanced UEBA • Advanced Analytics • CTO • SSPM • CSPM • Cloud Confidence Index (CCI) • NG-SWG

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(1)(ii)		Advanced User Entity and Behavior Analytics incorporates many more ML-based anomaly-detection models than Standard UEBA. It also includes the User Confidence Index, a dynamic, quantifiable risk score for each user based on their behavior over time, and can be leveraged to adapt policies and controls, and recommend security training, in order to detect and mitigate insider threats. UCI can also be integrated with Netskope's Cloud Exchange in order to share information about insider threats via the Netskope Cloud Risk Exchange. Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM also routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations. SSPM alerts provide step-by-step instructions for remediation, and it can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	
164.308(a)(2)	1. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Netskope does not map to this requirement.	

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(3)	i. 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. ii. (A) Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. ii. (B) Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. ii. (C) Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Netskope's Cloud Access Security Broker (CASB), Next-Gen Secure Web Gateway (NG-SWG), Data Loss Prevention (DLP) engine, and ZTNA Next can enforce Role-Based Access Controls to support organizational access management policies based on the principle of least privilege. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's NG-SWG integrates with NIST-compliant third party identity providers, extending SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's context-aware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Advanced User and Entity Behavior Analytics incorporates ML-based anomaly-detection models. It also includes the User Confidence Index, a dynamic, quantifiable risk score for each user based on their behavior over time, and can be leveraged to adapt policies and controls, and recommend security training, in order to detect and mitigate insider threats. UCI can also be integrated with Netskope's Cloud Exchange in order to share information about insider threats via the Netskope Cloud Risk Exchange.	• SD-WAN • ZTNA Next • DLP • NG-SWG • CASB • Advanced UEBA

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(4)	i. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. ii. (A) 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. ii. (B) 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. ii. (C) Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Netskope's Borderless SD-WAN permits network segmentation and allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availablility connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations. SSPM alerts provide step-by-step instructions for manual remediation, and can also be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	• SD-WAN • ZTNA Next • DLP • CTO • SSPM • CSPM

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(5)(i)	1. Implement a security awareness and training program for all members of its workforce (including management).	Netskope can assist communication and track acknowledgement of policies through pop-up banners and coaching pages across its products, notifying employees of potential policy infringements, requesting a justification for risky actions, suggesting alternatives, or referring users for further training on organizational or regulatory requirements. Advanced User and Entity Behavior Analytics incorporates many more ML-based anomaly-detection models than Standard UEBA. It also includes the User Confidence Index, a dynamic, quantifiable risk score for each user based on their behavior over time, and can be leveraged to adapt policies and controls, and recommend security training, in order to detect and mitigate insider threats. UCI can also be integrated with Netskope's Cloud Exchange in order to share information about insider threats via the Netskope Cloud Risk Exchange.	• Advanced UEBA • All products
164.308(a)(5)(ii)(A)	1. Implement periodic security updates.	Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's context-aware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization. Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	• Device Intelligence • CTO • SSPM • CSPM • Cloud Confidence Index (CCI) • NG-SWG

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(5)(ii)(A)		Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations, and provides step-by-step instructions for remediation. SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	
164.308(a)(5)(ii)(B)	1. Implement procedures for guarding against, detecting, and reporting malicious software.	Remote Browser Isolation is a built-in feature of Netskope's NG-SWG that isolates risky and uncharacterized web sites in a secure, cloud-based container or "sandbox" and prevents unauthorized software execution. Any malware is executed in the container and cannot infect the organization's network. Netskope's Standard Threat Protection protects against known malware, uses machine learning analysis to detect new malware, and provides real-time phishing detection, corroborative sandboxing, and web filtering. Netskope Threat Protection integrates with threat intelligence feeds from Netskope's Cloud Threat Exchange, and with other Netskope Intelligent Security Service Edge tools including Remote Browser Isolation, Cloud Firewall, and User Entity and Behavior Analytics to create a layered, defense-indepth security solution. In addition to the capabilities of Standard Threat Protection, Advanced Threat Protection incorporates deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect and protect against new malware. Advanced DLP includes IaaS Storage Scanning, which can discover malware hidden in cloud storage services and prevent it from infecting the organization's cloud environment. Beyond simple "allow" or "block" rules, NG-SWG's context-aware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions.	• RBI • Advanced DLP • Advanced Threat Protection • Threat Protection • Advanced UEBA • NG-SWG • CTO • SSPM • CSPM • Device Intelligence

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(5)(ii)(B)		Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations, and can provide step-by-step instructions for remediation. SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings. Advanced User Entity and Behavior Analytics incorporates many more ML-based anomaly-detection models than Standard UEBA. It also includes the User Confidence Index, a dynamic, quantifiable risk score for each user based on their behavior over time, and can be leveraged to adapt policies and controls, and recommend security training, in order to detect and mitigate insider threats. UCI can also be integrated with Netskope's Cloud Exchange in order to share information about insider threats via the Netskope Cloud Risk Exchange.	

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(5)(ii)(C)	1. Implement procedures for monitoring log-in attempts and reporting discrepancies.	Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next also integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Advanced User Entity and Behavior Analytics incorporates many more ML-based anomaly-detection models than Standard UEBA. It also includes the User Confidence Index, a dynamic, quantifiable risk score for each user based on their behavior over time, and can be leveraged to adapt policies and controls, and recommend security training, in order to detect and mitigate insider threats. UCI can also be integrated with Netskope's Cloud Exchange in order to share information about insider threats via the Netskope Cloud Risk Exchange.	• Advanced UEBA • NG-SWG • All products • SD-WAN • ZTNA Next
164.308(a)(5)(ii)(D)	1. Implement procedures for creating, changing, and safeguarding passwords.	Netskope's NG-SWG and ZTNA Next integrate with NISTcompliant third party identity providers, extending SSO/MFA across managed and unmanaged web and cloudbased apps and services. Both products can be configured to enforce organizational policies regarding password management.	• NG-SWG • ZTNA Next
164.308(a)(6)	i. Implement policies and procedures to address security incidents. 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 or business associate; and document security incidents and their outcomes.	Netskope NG-SWG, CASB, ZTNA Next, Cloud Firewall, and Cloud and SaaS Security Management can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope's Cloud Log Shipper exports event and alert logs from Netskope's NG-SWG, CASB, ZTNA Next, Cloud Firewall, and Cloud and SaaS Security Posture Management tools to the organization's SIEM or other incident response tool.	• SD-WAN • CLS • CTO • NG-SWG • CASB • ZTNA Next • Cloud Firewall • CSPM • SSPM • DLP

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(6)		Netskope's Cloud Ticket Orchestrator allows organizations to create rules that automatically generate service tickets and automate workflows in response to security alerts. Properly configured, Cloud Ticket Orchestrator can automate much of an organization's incident response and recovery plan, including enforcing role-based access controls for all teams and team members involved in incident response. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations.	
164.308(a)(7)	i. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. ii. (A) Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. ii. (B) Establish (and implement as needed) procedures to restore any loss of data. ii. (C) Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. ii. (D) Implement procedures for periodic testing and revision of contingency plans. ii. (E) Assess the relative criticality of specific applications and data in support of other contingency plan components.	Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Several Netskope products, including its CASB, NG-SWG, Advanced Analytics, and Cloud Confidence Index can help organizations identify and assess the relative criticality of specific business processes, applications, and data. Netskope's CASB and NG-SWG can identify and inventory both managed and unmanaged apps and cloud services to assist in determining the scope of any contingency plan testing. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope’s Cloud Confidence Index (CCI) provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor’s security policies and certifications, audit capabilities, legal and privacy concerns, and more.	• SD-WAN • DLP • Advanced Analytics • Cloud Confidence Index (CCI) • CASB • NG-SWG

Subsection	Requirements(s)	Netskope Response	Products
164.308(a)(8)	1. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Netskope's CASB can generate alerts and export them to the organization's Security Incident and Event Management tool to facilitate automated incident response and recovery; event logs can be leveraged to perform lessons learned and generate Progress and Action On Milestones reports. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations, and provides step-by-step instructions for remediation. SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	• CASB • CTO • SSPM • CSPM
164.308(b)(1)-(3)	1. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Netskope's CASB can assist with asset inventory, acquisition strategy, third party risk management, and business continuity planning by identifying and inventorying managed and unmanaged apps and cloud services in the organization's IT ecosystem, and assessing their criticality based on usage and risk level.	• CASB

SECTION 164.310 PHYSICAL SAFEGUARDS

While Netskope does not provide physical and environmental security tools, the Netskope platform provides logging and reporting, access management controls, and user and entity behavior analytics that complement the organization’s physical security controls.

Subsection	Requirements(s)	Netskope Response	Products
164.312(a)(1)	1. 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).	Netskope's NG-SWG and ZTNA Next integrate with NISTcompliant third party identity providers, extending SSO/ MFA across managed and unmanaged web and cloudbased apps and services. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations, and provides step-by-step instructions for remediation. SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	• All products • SD-WAN • ZTNA Next • DLP • CTO • SSPM • CSPM

Subsection	Requirements(s)	Netskope Response	Products
164.312(a)(2)(i)	1. Assign a unique name and/or number for identifying and tracking user identity.	Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere, enforcing uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations.	• SD-WAN • ZTNA Next • NG-SWG • CTO • SSPM • CSPM
164.312(a)(2)(ii)	1. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations and provide step-by-step instructions for remediation. SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	• SD-WAN • CTO • SSPM • CSPM

Subsection	Requirements(s)	Netskope Response	Products
164.312(a)(2)(iii)	1. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts.	• ZTNA Next
164.312(a)(2)(iv)	1. Implement a mechanism to encrypt and decrypt electronic protected health information.	Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles.	• DLP • ZTNA Next
164.312(b)	1. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's contextaware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope's CASB allows monitoring and logging of activities performed in SaaS and IaaS services - including information on user, device, instance, and action - and can apply activity-level and data loss prevention controls in real time, not just blocking an action but also requesting a business justification or providing training on organization policy. Netskope's Proactive Digital Experience Management provides end-to-end visibility into the user experience from endpoints to the cloud, enables automated troubleshooting, and allows administrators to proactively diagnose and mitigate performance issues.	• SD-WAN • CTO • Device Intelligence • CASB • NG-SWG • P-DEM • DLP

Subsection	Requirements(s)	Netskope Response	Products
164.312(b)		Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization. Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more. Netskope's Cloud Ticket Orchestrator allows organizations to create rules that automatically generate service tickets and automate workflows in response to security alerts. Properly configured, Cloud Ticket Orchestrator can automate much of an organization's incident response and recovery plan, including enforcing role-based access controls for all teams and team members involved in incident response. Cloud Ticket Orchestrator is a component of Netskope's Cloud Exchange, which is a standard feature of every Netskope deployment.	
164.312(c)(1)	1. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's CASB allows monitoring and logging of activities performed in SaaS and IaaS services - including information on user, device, instance, and action - and can apply activity-level and data loss prevention controls in real time, not just blocking an action but also requesting a business justification or providing training on organization policy.	• DLP • CTO • SSPM • CSPM • NG-SWG • CASB

Subsection	Requirements(s)	Netskope Response	Products
164.312(c)(1)		NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's contextaware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations.	
164.312(c)(2)	1. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Netskope NG-SWG and CASB's detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations, and provides step-by-step instructions for remediation.	• DLP • CTO • SSPM • CSPM • NG-SWG • CASB

Subsection	Requirements(s)	Netskope Response	Products
164.312(d)	1. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more.	• SD-WAN • ZTNA Next • NG-SWG
164.312(e)	1. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. 2. (i) Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. 3. (ii) Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Netskope's Data Loss Prevention engine provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Netskope's NG-SWG integrates with NIST-compliant third party identity providers, and extends SSO/MFA across managed and unmanaged web and cloud-based apps and services. NG-SWG can decode and log over one hundred inline activities, and develops a baseline of user activity in order to detect anomalous behavior, applying granular policy controls based on the nature of the activity or data being transmitted, or the particular app instance being used. Beyond simple "allow" or "block" rules, NG-SWG's context-aware controls can respond to risky or anomalous behavior by requiring a stepped-up multi-factor authentication, or notifying the user of a potential policy violation and requesting a business justification, suggesting a safer alternative, or referring the user to third-party vendors for just-in-time cybersecurity training.	• SD-WAN • ZTNA Next • NG-SWG • DLP

Subsection	Requirements(s)	Netskope Response	Products
164.312(e)		Netskope NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more.	

SECTION 164.314 ORGANIZATIONAL REQUIREMENTS

164.314(a)	1. (This subsection mandates the inclusion of certain provisions in the contracts between covered entities and business associates, and between business associates and subcontractors)	Netskope's CASB and NG-SWG can identify and inventory both managed and unmanaged apps and cloud services to assist in determining which vendors may require contract measures to be put in place to appropriately safeguard information.	• NG-SWG • CASB
164.314(b)	1. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Several Netskope products, including its CASB, NGSWG, Advanced Analytics, and Cloud Confidence Index, can assist the organization in identifying important third parties and assessing their cybersecurity maturity. Netskope's CASB and NG-SWG can identify and inventory both managed and unmanaged apps and cloud services to assist in determining the scope of any contingency plan testing. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope's Cloud Confidence Index (CCI) provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	• CASB • NG-SWG • Advanced Analytics • Cloud Confidence Index (CCI) • CSPM • SSPM • CTO

Subsection	Requirements(s)	Netskope Response	Products
164.314(b)	2. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to - i. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; ii. Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; iii. Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and iv. Report to the group health plan any security incident of which it becomes aware.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. CSPM also routinely scans cloud storage buckets to prevent data exfiltration, and can be integrated with Netskope's Cloud Ticket Orchestrator, allowing it to send alerts and automate remediation efforts. Netskope's SaaS Security Posture Management (SSPM) continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations. SSPM alerts provide step-by-step instructions for remediation, and SSPM can be integrated with Netskope's Cloud Ticket Orchestrator to generate service tickets from alerts and automate remediation efforts. Previously detected misconfigurations can be converted into new rules, improving security based on findings.	

SECTION 164.316 POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

164.316(a)	1. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart. 2. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Netskope can enforce organizational policies defined by the organization. Netskope additionally can assist communication and track acknowledgement of policies through implementation of pop-up banners/coaching pages across its product that can notify employees of potential policy infringements in line with organizational requirements	• All products

Subsection	Requirements(s)	Netskope Response	Products
164.316(b)(1)	i. Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form. ii. If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Netskope can assist communication and track acknowledgement of policies through implementation of pop-up banners and coaching pages across its products that can notify employees of potential policy infringements in line with organizational requirements. Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent similar misconfigurations. Previously detected misconfigurations can be converted into new rules, improving security based on findings. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted.	• All products • CSPM • SSPM
164.316(b)(2)	i. Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. ii. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. iii. Review documentation periodically, and update as needed, in response to environmental or operational changesaffecting the security of the electronic protected health information.	Netskope's Cloud Security Posture Management continuously monitors an organization's mission critical IaaS platforms to prevent misconfigurations, including deviations from organizational access management policies, or from regulatory and industry standards, ensuring these platforms and associated data are being used consistent with their intended purpose. Netskope's SaaS Security Posture Management continuously monitors an organization's mission critical SaaS functions to prevent siilar misconfigurations. Several Netskope products, including its CASB, NGSWG, Advanced Analytics, and Cloud Confidence Index can help organizations identify and assess the relative criticality of specific business processes, applications, and data, making it easier to update security policies in light of changes to the organization's IT ecosystem. Netskope's CASB and NG-SWG can identify and inventory both managed and unmanaged apps and cloud services to assist in determining the scope of any contingency plan testing. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted.	• All products • CTO • SSPM • CSPM

Subsection	Requirements(s)	Netskope Response	Products
164.316(b)(2)		Netskope's Cloud Confidence Index (CCI) provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	

Disclaimer

The content provided has been created to the best of Netskope's ability and knowledge. However, Netskope cannot guarantee the accuracy, completeness, or timeliness of the information. Netskope is not liable for any errors or omissions in the content, and readers are encouraged to verify the information independently. The use of this content is at the reader's own risk, and Netskope shall not be held responsible for any consequences resulting from reliance on the provided information.

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.