Nylas
Type 1 Attestation
(AT-C 105 and AT-C 205)
HIPAA/HITECH
2020

Table of Contents

SECTION 1 ASSERTION OF NYLAS MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 NYLAS' DESCRIPTION OF ITS E-MAIL, CALENDAR, AND CONTACT MANAGEMENT SERVICES SYSTEM AS OF AUGUST 31, 2020 6

OVERVIEW OF OPERATIONS 7
Company Background 7
Description of Services Provided 7
Principal Service Commitments and System Requirements 8
Components of the System 9
Boundaries of the System 11
HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS 11
Changes to the System in the Last 12 Months 14
Incidents in the Last 12 Months 14
Requirements Not Applicable to the System 14
Subservice Organizations 15
Complementary User Entity Controls 16
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 18
ADMINISTRATIVE SAFEGUARDS 18
PHYSICAL SAFEGUARDS 28
TECHNICAL SAFEGUARDS 30
ORGANIZATIONAL REQUIREMENTS 33
BREACH NOTIFICATION 36
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 42

SECTION 1

ASSERTION OF NYLAS MANAGEMENT

ASSERTION OF NYLAS MANAGEMENT

September 28, 2020

We have prepared the description of Nylas' health information security program for the E-mail, Calendar, and Contact Management Services System (the "description") for user entities of the system as of August 31, 2020. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the E-mail, Calendar, and Contact Management Services System as of August 31, 2020. The criteria we used in making this assertion were that the description:
    i. fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the E-mail, Calendar, and Contact Management Services System
    ii. describes the specified controls within the security program designed to achieve the security program's objectives
    iii. does not omit or distort information relevant to the health information security program for the E-mail, Calendar, and Contact Management Services System and may not include every aspect that an individual user entity may consider important in its own particular environment

b. The health information security program governing the E-mail, Calendar, and Contact Management Services System includes essential elements of HIPAA and HITECH. The criteria we used in making this assertion were that:
    i. management determined the applicable controls (the "controls") included in the health information security program
    ii. the controls documented met the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
        - Administrative Safeguards
        - Physical Safeguards
        - Technical Safeguards
        - Organizational Requirements
        - Breach Notification

Section 3 of this report includes Nylas' description of the health information security program for the E-mail, Calendar, and Contact Management Services System that is covered by this assertion.

David Ting

David Ting
Vice President of Engineering
Nylas

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Nylas

We have examined Nylas' assertion that the description of its health information security program for the Nylas' E-mail, Calendar, and Contact Management Services System listed in Section 3 (the "description") provided to user entities as of August 31, 2020, is fairly presented and that the health information security program governing the E-mail, Calendar, and Contact Management Services System includes essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009, is presented in accordance with the criteria set forth in Nylas' assertion in Section 1. Nylas' management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Nylas uses Amazon Web Services ('AWS' or 'subservice organization') for cloud hosting services. The description indicates that certain applicable HIPAA/HITECH requirements can only be met if controls at the subservice organization are suitably designed. The description presents Nylas' system; its controls relevant to the applicable HIPAA/HITECH requirements; and the types of controls that the service organization expect to be implemented, and suitably designed at the subservice organization to meet certain applicable HIPAA/HITECH requirements. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design of Nylas' health information security program for the E-mail, Calendar, and Contact Management Services System and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

A-LIGN ASSURANCE did not perform procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions relevant to meet the applicable HIPAA/HITECH requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable HIPAA/HITECH requirements is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in Nylas' assertion in Section 1:

a. The description fairly presents the health information security program for the E-mail, Calendar, and Contact Management Services System that was designed and implemented as of August 31, 2020; and
b. The health information security program governing the E-mail, Calendar, and Contact Management Services System includes essential elements of HIPAA and HITECH.

This report and the description of tests of controls and results thereof are intended solely for the information and use of Nylas; user entities of Nylas' E-mail, Calendar, and Contact Management Services System as of August 31, 2020; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations

- Complementary user-entity controls and complementary subservice organization controls and how they interact with related controls at the service organization to meet the HIPAA security program
- The HIPAA security program
- The risks that may threaten the achievement of the HIPAA security program and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
September 28, 2020

SECTION 3

NYLAS' DESCRIPTION OF ITS E-MAIL, CALENDAR, AND CONTACT MANAGEMENT SERVICES SYSTEM AS OF AUGUST 31, 2020

OVERVIEW OF OPERATIONS

Company Background

Nylas was co-founded at MIT in 2013 by Nylas Chief Technology Officer (‘CTO’), Christine Spang. The Universal APIs in the Nylas communications platform allow developers to leverage complex, unstructured data and integrate it into applications. With a few lines of code, developers can build features that bi-directionally syncs data and integrates with user’s e-mail, calendar, and contacts books.

Tens of thousands of developers across more than 22 countries use Nylas to embed communications into their platforms.

Description of Services Provided

Nylas provides E-mail, Calendar, and Contact Management Services throughout the United States. The Company was founded to provide productivity infrastructure services to medical software solutions and CRM companies.

Nylas' core application, api.nylas.com, is a multiuser, transaction-based application suite that enables the syncing of data when developers need E-mail, Calendar and Contact Management Services during integration. Nylas enables processing of the following tasks related to communication:

- E-mail API:
  Get bi-directional integration with users’ inboxes. Embed full e-mail features within the application
- Calendar API:
  Sync users’ calendars with customer’s application to schedule events, send meeting invitations, RSVP, and more
- Contacts API:
  Easily integrate customer users’ address books. Leverage rich contact info with full contacts sync

Customers can control the exact data types and fields that are stored within Nylas:

Nylas Scope	Description
e-mail.modify	Read and modify all messages, threads, file attachments, and read e-mail metadata like headers. Does not include send.
e-mail.read_only	Read all messages, threads, file attachments, drafts, and e-mail metadata like headers-no write operations.
e-mail.send	Send messages only. No read or modify privileges on users' e-mails.
e-mail.folders_and_labels	Read and modify folders or labels, depending on the account type.
e-mail.metadata	Read e-mail metadata including headers and labels/folders, but not the message body or file attachments.
e-mail.drafts	Read and modify drafts. Does not include send.
calendar	Read and modify calendars and events.
calendar.read_only	Read calendars and events.
room_resources.read_only	Read available room resources for an account.

Nylas Scope	Description
contacts	Read and modify contacts.
contacts.read_only	Read contacts.

Electronic Protected Health Information (ePHI) Transmission, Processing & Reporting:

Nylas process e-mails, calendars and Contacts data. Information is shared and secured with the latest HTTPS and TLS protocol in transit and cached for 2 weeks by default. Clients have the ability to set retention policy to increase/decrease the retention period based on internal security requirements. Data would be stored in secured places and encrypted. Accessing the data would require authentication and authorization.

Principal Service Commitments and System Requirements

Nylas designs its processes and procedures related to E-mails, Calendars & Contacts to meet its objectives for its API integration services. Those objectives are based on the service commitments that Nylas makes to user entities, the laws and regulations that govern the provision of E-mail/Calendar/Contacts API integration services, and the financial, operational, and compliance requirements that Nylas has established for the services. The E-mail/Calendar/Contacts integration services of Nylas are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Nylas operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the API integration that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Nylas establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Nylas' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the API integration.

Components of the System

Infrastructure

Primary infrastructure used to provide E-mail, Calendar, and Contact Management Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
All system, security, and network infrastructure are hosted on EC2, S3, Kinesis and other Amazon services	AWS	Serving the Nylas API

Software

Primary software used to provide E-mail, Calendar, and Contact Management Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Sync Engine	Debian Linux	Providing the Nylas API

People

The Nylas staff provides support for the above services in each of the following functional areas:

- Leadership team - provides general oversight and strategic planning of operations
- Software Engineers - responsible for delivering a responsive system that fully complies within specifications
- Site Reliability Engineers - responsible for effective provisioning, installation/configuration, operation, and maintenance of applications relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Nylas in delivering its API. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, Intrusion Detection System (‘IDS’) alerts, or automated patching systems
- Incident reports documented via Dropbox Paper documents

Data, as defined by Nylas, constitutes the following:

- E-mails
- Calendar
- Contacts

This data is available in electronic formats, such as comma-delimited value file exports, or electronically from the various websites. The availability of this data is limited by job function. Data delivered externally will only be sent using a secure method-encrypted e-mail, secure FTP, or secure websites-to business partners who will be using Nylas-developed websites or over connections secured by trusted security certificates. Nylas uses Transport Layer Security to encrypt data exchanges with all partners.

Health Information Security Program Processes, Policies and Procedures

Nylas has developed a health information security management program to meet the information security and compliance requirements related to E-mail/Calendar/Contact API integration services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that Nylas has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show how Nylas complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at predefined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems are restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Requirements - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required.

Boundaries of the System

The scope of this report includes the E-mail, Calendar, and Contact Management Services System performed in the San Francisco, California; New York, New York; Denver, Colorado; and Toronto, Ontario facilities.

This report does not include the cloud hosting services provided by AWS at multiple US facilities.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

Nylas' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Nylas' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Risk Assessment Process

Nylas' risk assessment process identifies and manages risks that could potentially affect Nylas' ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Nylas identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Nylas, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Nylas has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Nylas attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Nylas' E-mail/Calendar/Contact API Integration system; as well as the nature of the components of the system result in risks that the safeguards will not be met. Nylas addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the safeguards are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the safeguards and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Nylas' management identifies the specific risks that the safeguards will not be met and the controls necessary to address those risks.

Periodic Assessments

Nylas has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by Nylas to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Chief Security Officer ('CSO') at periodic intervals:

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality
- *Health Information Security Risks*: Health information security risks are assessed by the CSO. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CSO of the organization

Periodic Testing and Evaluation

Nylas completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Information and Communications Systems

Information and communication are an integral component of Nylas' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Nylas, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Nylas personnel via e-mail messages.

Specific information systems used to support Nylas' API Integration system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Nylas' management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Nylas' management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Nylas' operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Nylas' personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all Nylas personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity

- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

Nylas employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

Incident Response

Nylas maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

Remediation and Continuous Improvement

Areas of non-compliance in Nylas' internal control system surface from many sources, including the Company’s ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and makes the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company’s procedures or personnel.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the review date.

Requirements Not Applicable to the System

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative	164.308(a)(4)(ii)(A)	The entity is not a health care clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
	164.308(b)(2)	The entity does not use subcontractors. The organization would not share ePHI if it was in their possession.

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Physical	164.310(c)	The entity is not a covered entity.
Organizational	164.314(a)(1)	
	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1)	The entity is not a plan sponsor.
	164.314(b)(2)	The entity is not a group health plan.

Breach Notification	164.402;
	164.404(a);
	164.404(b);
	164.404(c)(1);
	164.404(c)(2);
	164.404(d)(1)(i);
	164.404(d)(1)(ii);
	164.404(d)(2);
	164.404(d)(2)(i);
	164.404(d)(2)(ii);
	164.404(d)(3);
	164.406;
	164.408(a);
	164.408(b);
	164.408(c)
		The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple US facilities.

Subservice Description of Services

AWS is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. In aggregate, these cloud computing web services provide a set of primitive abstract technical infrastructure and distributed computing building blocks and tools.

Complementary Subservice Organization Controls

Nylas' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the safeguards related to Nylas' services to be solely achieved by Nylas control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nylas.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the safeguards are met:

Subservice Organization Controls - AWS		
Safeguard / Procedure	**Requirement**	**Applicable Controls**
Administrative	164.308(a)(7)(ii)(A)	An automated backup system is utilized to perform scheduled system backups.

Subservice Organization Controls - AWS		
Safeguard / Procedure	**Requirement**	**Applicable Controls**

	164.308(a)(7)(ii)(B);
	164.308(a)(7)(ii)(C);
	164.308(a)(7)(ii)(D);
	164.308(a)(8)
		Business continuity and disaster recovery plans are tested on an annual basis.

Physical	164.310(a)(1);
	164.310(a)(2)(ii);
	164.310(a)(2)(iii)
		Physical access to facilities housing the production servers is restricted to authorized personnel.

	164.310(a)(2)(i)	Business continuity and disaster recovery plans are tested on an annual basis.
	164.310(a)(2)(iv)	Repairs and modifications to the physical components of a facility housing production systems are documented.
Technical	164.312(a)(2)(ii)	Business continuity and disaster recovery plans are tested on an annual basis.

Nylas management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant safeguards through written contracts, such as service level agreements. In addition, Nylas performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

Complementary User Entity Controls

Nylas' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Safeguards related to Nylas' services to be solely achieved by Nylas control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nylas'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Safeguards described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Nylas.
2. User entities are responsible for notifying Nylas of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Nylas services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Nylas services.
6. User entities are responsible for providing Nylas with a list of approvers for security and system configuration changes for data transmission.

7. User entities are responsible for immediately notifying Nylas of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Inspected the incident response policies and procedures to determine documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding preventing, detecting, containing, and correcting security violations. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An intrusion prevention system ('IPS') is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. File integrity monitoring ('FIM') software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Vulnerability scans are performed weekly on the environment to identify control gaps and vulnerabilities.
	Network	
		Network user access is restricted via role based security privileges defined within the access control system.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network audit logs are maintained and reviewed annually.
	Database	
		Database user access is restricted via role based security privileges defined within the access control system. Database audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Database audit logs are maintained and reviewed annually.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system. Application audit logging settings are in place that include: • Account logon events • Page Views • User events • Group Events Application audit logs are maintained and reviewed annually.
164.308 (a)(1)(ii)(A)	**Risk analysis:** 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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Addressing the associated risks identified for each identified vulnerability
164.308 (a)(1)(ii)(B)	**Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Addressing the associated risks identified for each identified vulnerability Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Mitigate the risk • Accept the risk • Transfer the risk • Avoid the risk • Exclude the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Vulnerability scans are performed weekly on the environment to identify control gaps and vulnerabilities. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Disciplinary policies, which include warnings, suspension, and termination, are in place for employee misconduct.
	Network	
164.308 (a)(1)(ii)(D)	**Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Network audit logging settings are in place that include: • Account logon events • Page Views • User events • Group Events Network audit logs are maintained and reviewed as-needed.
	Database	
		Database audit logging settings are in place that include: • Account logon events • Page Views • User events • Group Events Database audit logs are maintained and reviewed as-needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		Application audit logging settings are in place that include: - Account logon events - Page Views - User events - Group Events Application audit logs are maintained and reviewed as-needed.
164.308 (a)(2)	**Assigned security responsibility:** 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.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected electronic protected health information ('ePHI') is formally documented and assigned to a job role.
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Policies and procedures are formally defined and documented regarding accessing ePHI. Network user access is restricted via role based security privileges defined within the access control system.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** 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.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Logical access to systems is approved and granted to an employee as a component of the hiring process.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Policies and procedures are formally defined and documented regarding accessing ePHI. Network user access is restricted via role based security privileges defined within the access control system.
164.308 (a)(3)(ii)(C)	**Termination procedures:** 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) [the Workforce Clearance Procedure] of this section.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Logical access to systems is revoked as a component of the termination process.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** 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.	Not applicable - The entity is not a healthcare clearinghouse.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Logical access to systems is approved and granted to an employee as a component of the hiring process.
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** 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.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Employees are required to attend continued training that relates to their job role and responsibilities. Upon hire, employees are required to complete information security and awareness training. Current employees are required to complete information security and awareness training on an annual basis.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Policies and procedures are formally documented regarding preventing, detecting, and reporting the presence of malicious software. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Network	
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Network audit logging configurations are in place that include: • Account logon events • Page Views • User events • Group Events Network audit logs are maintained and available for review, as-needed.
	Database	
		Database audit logging settings are in place that include: • Account logon events • Page Views • User events • Group Events Database audit logs are maintained and reviewed as-needed.
	Application	
		Application audit logging settings are in place that include: • Account logon events • Page Views • User events • Group Events Application audit logs are maintained and reviewed as-needed.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords.
	Network	
		Network user access is restricted via role based security privileges defined within the access control system.
	Database	
		Database user access is restricted via role based security privileges defined within the access control system.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system.
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(6)(ii)	**Response and reporting:** 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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. Resolution of incidents are documented within the ticket and communicated to affected users.
164.308 (a)(7)(i)	**Contingency plan:** 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 ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Data backup policies and procedures are formally documented. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.308 (a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Addressing the associated risks identified for each identified vulnerability
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirement.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	Not applicable - The entity is not a covered entity.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	Not applicable - The entity does not use subcontractors. The organization would not share ePHI if it was in their possession.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business continuity and disaster recovery plans are tested on an annual basis. Data backup restoration tests are performed at least annually. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Not applicable - The entity is not a covered entity.
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. Data that is no longer required for business purposes is rendered unreadable.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	The entity sanitizes media containing ePHI when the media is to be re-used. Data that is no longer required for business purposes is rendered unreadable.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Data backup policies and procedures are formally documented. Full backups of certain application and database components are performed on a monthly basis and incremental backups are performed on a daily basis.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Standardized user access request tickets are utilized to request access to ePHI. Access must be approved prior to access being granted. A valid public key is required to be granted access to the operating system. Network administrative access is restricted to user accounts accessible by authorized personnel. Termination procedures require the removal of employee access to ePHI upon termination of employment.
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers. A valid public key is required to be granted access to the operating system. Network devices are configured to log events and access attempts to ensure that system activity can be traced to a specific user and that necessary data is available in the system logs to support audit and other related business functions.
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The disaster recovery plan is tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after a five-minute period of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Secure socket layer (‘SSL’), secure file transfer program (‘SFTP’), and other encryption technologies are used for defined points of connectivity.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Data is stored in encrypted format using software supporting the advanced encryption standard (‘AES’).
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Network audit policy configurations are in place that include: • Account logon events • Page views • User events • Group events Network logs are generated by management and are reviewed as necessary.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Formal policy and procedure documents are in place to protect ePHI from improper alteration or destruction. A valid public key is required to be granted access to the operating system. Network audit policy configurations are in place that include: • Account logon events • Page views • User events • Group events Network logs are generated by management and are reviewed as necessary. SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	SSL, SFTP, and other encryption technologies are used for defined points of connectivity. Data is stored in encrypted format using software supporting the AES.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. A valid public key is required to be granted access to the operating system.
	Network	
		A valid public key is required to be granted access to the operating system.
	Database	
		Databases are configured to enforce password requirements that include: • Password history • Password length

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		A valid public key is required to be granted access to the application.
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	SSL, SFTP, and other encryption technologies are used for defined points of connectivity. Data is stored in encrypted format using software supporting the AES. Network audit policy configurations are in place that include: • Account logon events • Page views • User events • Group events
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	SSL, SFTP, and other encryption technologies are used for defined points of connectivity. Data is stored in encrypted format using software supporting the AES.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	Not applicable - The entity is not a covered entity.
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health…; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	Not applicable - The entity is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI 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 ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not applicable - The entity is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** 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 ePHI 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, including a subcontractor, 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.	Not applicable - The entity is not a group health plan.
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. 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.	The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers. The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (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.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later. Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel. Policies and procedures are created and maintained in written and electronic form.
164.316 (b)(1)(ii)	**Documentation:** 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.	HIPAA related incidents and events are documented in a ticketing system.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(2)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later.
164.316 (b)(2)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.
164.316 (b)(2)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)	**Substitute notice**. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not applicable - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION

Ref	Regulation	Control Activity Specified by the Service Organization
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject's records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual who's unsecured ePHI has been accessed during the breach is disclosed during notification procedures.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.
164.414	**Administrative requirements and burden of proof**: (a) covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart. (b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Nylas was limited to the HIPAA/HITECH requirements and related control activities specified by the management of Nylas and did not encompass all aspects of Nylas' operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

TEST	**DESCRIPTION**
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements;
- Understand the flow of ePHI through the service organization;
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented.