



Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Assessment Report

Company Name: Cisco

Audit Guideline - NIST Special Publication 800-66 Revision 1

Assessment Period: 1st November 2023 to 27th December 2023

Report Date: 23rd January 2024

Auditor: Coral eSecure Limited

2010 Winston Park Drive

Suite# 200 Oakville, ON

L6H 5R7 Canada

Table of Contents

1. Assertion of CISCO Management	3
2. Auditor Assertion by Coral eSecure	4
3. Assessment Summary	5
4. Audit Scope and Methodology	6
5. Detail Assessment Results	8
Administrative Safeguards	9
1. Security Management Process (§ 164.308(a)(1))	9
2. Assigned Security Responsibility (§ 164.308(a)(2))	12
3. Workforce Security (§ 164.308(a)(3))	13
4. Information Access Management (§ 164.308(a)(4))	14
5. Security Awareness and Training (§ 164.308(a)(5))	15
6. Security Incident Procedures (§ 164.308(a)(6))	16
7. Contingency Plan (§ 164.308(a)(7))	17
8. Evaluation (§ 164.308(a)(8))	19
9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))	21
Physical Safeguards	22
10. Facility Access Controls (§ 164.310(a)(1))	22
11. Workstation Use (§ 164.310(b))	23
12. Workstation Security (§ 164.310(c))	24
13. Device and Media Controls (§ 164.310(d)(1))	25
Technical Safeguards	26
14. Access Control (§ 164.312(a)(1))	26
15. Audit Controls (§ 164.312(b))	29
16. Integrity (§ 164.312(c)(1))	30
17. Person or Entity Authentication (§ 164.312(d))	32
18. Transmission Security (§ 164.312(e)(1))	34
Organizational Requirements	35
19. Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))	35
20. Requirements for Group Health Plans (§ 164.314(b)(1))	36
Policies and Procedures and Documentation Requirements	37
21. Policies and Procedures (§ 164.316(a))	37
22. Documentation (§ 164.316(b)(1))	37

1. Assertion of CISCO Management

We have designed, documented and implemented the requirements for the HIPAA Security Rule as per NIST Special Publication 800-66 Revision 1 based on the assessment of applicable requirements.

During the implementation journey, we went through the following process:

- Understanding individual HIPAA requirements, and those that apply to us.
- Documentation of policies, procedures and practices
- Allocation of roles and responsibilities
- Remediation of identified risks, and gaps
- Ongoing control monitoring

We understand that this is an ongoing process and we are committed to maintaining the program with new changes as and when we identify them.

We seek Coral's independent assessment of the design, implementation and effectiveness of the applicable requirements.

Users of this report may contact the undersigned for further questions.

DocuSigned by:

ADEE1D470032478...

Name: Richard Ward

Designation: Leader, Information Security



2. Auditor Assertion by Coral eSecure

We have performed the agreed-upon procedures enumerated below, which were agreed with CISCO based on applicable HIPAA requirements.

The procedures performed and results thereof are included in section 5 – Detail Assessment Results.

While every effort is made to ensure the accuracy and completeness of the information contained herein with respect to HIPAA, the choice of applicable requirements is based on the decisions applied by CISCO and the audit judgments are based on evidence provided by CISCO to Coral. CISCO is responsible for its compliance with those requirements.

Coral takes no responsibility and assumes no liability for any error/ omission or accuracy of the information other than what was provided to them for their review.

DocuSigned by:
Probal Choudhuri
F83AF8D999BA4CD...

Probal Choudhuri, CISSP, CISA, CISM, CDPSE
Principal Consultant (Director)
Coral eSecure Limited



3. Assessment Summary

Cisco aims to demonstrate that all three of its platforms, namely Campaign, Connect, and Engage HIPAA Security Rule compliance.

Coral has assessed Cisco's state of internal controls based on NIST Special Publication 800-66 Revision 1 –which provides detailed implementation and assessment requirements for implementing HIPAA Security Rules.

Coral has provided its opinion on each of the requirements based on the controls specified by Cisco and supporting evidence to fulfill those requirements.

The report is divided into the following subsections:

- Audit Scope and Methodology
- Detail Assessment Result

4. Audit Scope and Methodology

Audit Scope

The scope of the assessment covers the following:

- Webex Campaign v6.8
- Webex Engage v5.5
- Webex Connect v6.4.0
- Cloud Infrastructure Controls at AWS
- Cloud Infrastructure Controls at Azure Data Centre

Auditee Location

The audit was performed remotely.

Audit Methodology

The audit methodology included performing the following task:

- Understanding the relevance of HIPAA compliance in the organisation
- Interviews with staff associated with security.
- Policy, procedure and control verifications related to the given control area
- Configuration checks related to the application and associated security domains

Interviews

The following members of staff were interviewed during the engagement:

Name/s	Organisation/HIPAA Program Role
Kiran Reddy Angitipalli	Leader, Information Security

Policies and Procedure

The assessment covered reviewing the following documents and their associated artifacts to demonstrate Cisco complies with the required implementations.

- Webex campaign security overview.pdf
- Webex connect security overview.pdf
- Webex engage security overview.pdf
- Webex_cpaas_solutions_product_sheet_webex_engage
- Business_impact_analysis
- Cisco-secure-development-lifecycle
- FY23-code-of-business-conduct-english
- IMIEU-ISMS-ISP-02 Change management
- IMIEU-ISMS-POL-12 Access control policy

5. Detail Assessment Results

This section is further divided into the following HIPAA Security Rule requirements:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Safeguards
- Organisational Requirements
- Policies and Procedures and Documentation Requirements

Each of the 106 requirements from the NIST guide has been provided with the following information:

- HIPAA Requirement – This is aligned with NIST Special Publication 800-66 Revision 1
- Controls Specified by the organisation
- Evidence Demonstrated – This combines documentation, configuration, and records, as relevant to the control requirement
- Auditor Opinion

Administrative Safeguards

1. Security Management Process (§ 164.308(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
1. Identify Relevant Information Systems	- CISCO maintains an asset master that lists all forms of assets used for data processing. - Assets include software code and configuration assets located on the cloud. - CISCO Connect, CISCO Engage and CISCO Campaign - all are hosted in cloud infrastructure in AWS and Azure in US locations. - ePHI data is in databases that support these applications	Latest BIA report listing all assets that include, resources, applications, vendors, and office locations. Cisco SDLC Policy Platform specific documentation	No deviation noted
2. Conduct Risk Assessment	Cisco has a risk assessment and risk management program that: - Assess risks - Prioritizes risks - Mitigates risk - Master list of risk summary - Sample Identified risk - Sample mitigated risk - Risk lifecycle - communication, approval and mitigation	Cisco Internal Website Link showing risk register Cisco SDLC Policy	No deviation noted
3. Implement a Risk Management Program	Cisco has a risk assessment and risk management program that: - Assess risks - Prioritizes risks - Mitigates risk - Master list of risk summary - Sample identified risk - Sample mitigated risk - Risk lifecycle - communication, approval and mitigation	Cisco Internal Website Link showing risk register Cisco SDLC Policy	No deviation noted
4. Acquire IT Systems and Services	- Change management processes are in place that ensures acquisition of new systems and services are subject to approvals after consideration of business and security impact. - All changes to the cloud infrastructure are performed using a ticketing tool (Service now) that shows the history of requests and associated approvals per ticket.	Procedure - Change Management	No deviation noted



5. Create and Deploy Policies and Procedures	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies address security as part of the platform and the underlying infrastructure. These policies are subject to annual review.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview	No deviation noted
6. Develop and Implement a Sanction Policy	- A formal disciplinary or sanction policy is established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures. - Cisco Global Export Trade is dedicated to sanctions compliance and is responsible for the appropriate sanctions policies, procedures, monitoring and stakeholder reporting. Cisco's Investigations team independently obtains accurate and reliable information to discover the truth about reported employee-related alleged business conduct violations, such as financial fraud, illegal acts, control breaches with potential impact on financial reporting, and violations of COBC policies. - Depending on the nature of an alleged business conduct violation, the Ethics Office, the Legal Department, Human Resources, or other applicable organizations will promptly address the concern. - Should the concern warrant disciplinary action, Cisco will apply action in a consistent manner appropriate to the nature of the violation up to and including termination of employment if the circumstances warrant.	FY23 Code of Business Conduct There has been no case of disciplinary action	No deviation noted



7. Develop and Deploy the Information System Activity Review Process	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
8. Develop Appropriate Standard Operating Procedures	- CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. - These policies are subject to annual review.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
9. Implement the Information System Activity Review and Audit Process	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted

2. Assigned Security Responsibility (§ 164.308(a)(2))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
10. Select a Security Official To Be Assigned Responsibility for HIPAA Security	- A dedicated role of HIPAA Security Officer (Richard Ward) is in place.	HIPAA Security Officer – Responsibilities	No deviation noted
11. Assign and Document the Individual's Responsibility	- A dedicated role of HIPAA Security Officer is in place, who has documented responsibilities for HIPAA compliance.	HIPAA Security Officer – Responsibilities	No deviation noted

3. Workforce Security (§ 164.308(a)(3))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
12. Implement Procedures for Authorization and/or Supervision	- CISCO has a documented access control policy. - New employees/Users are provided access to the systems as part of standard HR employment formalities. - Any privilege access is subject to approval by work supervisor. - Temporary access is subject to automated or manual revocation procedure. - As part of separation policies, an employee's access is revoked.	Access Control Policy User registration communication System wise access control list that has systems and users Independent party access reports	No deviation noted
13. Establish Clear Job Descriptions and Responsibilities	- All employees have documented security responsibilities as part of the joining formalities.	SOC 2 Report - Policy extract	No deviation noted
14. Establish Criteria and Procedures for Hiring and Assigning Tasks	- Hiring of new employees is subject to the fulfillment of defined criteria that includes job descriptions, that includes technical and non-technical requirements.	SOC 2 Report - Policy extract	No deviation noted
15. Establish a Workforce Clearance Procedure	- Hiring of new employees is subject to the fulfillment of defined criteria that includes job descriptions, that includes technical and non-technical requirements.	SOC 2 Report - Policy extract	No deviation noted
16. Establish Termination Procedures	- Cisco has documented policy involving separation.	SOC 2 Report - Policy extract	No deviation noted

4. Information Access Management (§ 164.308(a)(4))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
17. Isolate Healthcare Clearinghouse Functions	Cisco is not Healthcare Clearinghouse – therefore not applicable		Not Applicable
18. Implement Policies and Procedures for Authorizing Access	CISCO has a documented access control policy. - Attached the access control policy and sample request process - Jira ticket	Access control policy Sample request process - Jira ticket	No deviation noted
19. Implement Policies and Procedures for Access Establishment and Modification	- CISCO has a documented access control policy. - New employees/Users are provided access to the systems as part of standard HR employment formalities. - Any privilege access is subject to approval by work supervisor. - Temporary access is subject to automated or manual revocation procedure. - All access to IT infrastructure is subject to an independent reporting. - As part of separation policies, an employee's access is revoked.	Access Control Policy User registration communication System wise access control list that has systems and users Independent party access reports	No deviation noted
20. Evaluate Existing Security Measures Related to Access Controls	- CISCO has a documented access control policy. - New employees/Users are provided access to the systems as part of standard HR employment formalities. - Any privilege access is subject to approval by work supervisor. - Temporary access is subject to automated or manual revocation procedure. - All access to IT infrastructure is subject to an independent reporting. - As part of separation policies, an employee's access is revoked.	Access Control Policy Guidelines for Risk Assessment and Risk Treatment HIPAA Risk register Access Review Record	No deviation noted

5. Security Awareness and Training (§ 164.308(a)(5))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
21. Conduct a Training Needs Assessment	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	SOC 2 Report - Policy extract Sample Employee training calendar	No deviation noted
22. Develop and Approve a Training Strategy and a Plan	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	SOC 2 Report - Policy extract Sample Employee training calendar	No deviation noted
23. Protection from Malicious Software; Log-in Monitoring; and Password Management Implementation Specifications (All Addressable)	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	SOC 2 Report - Policy extract Sample Employee training calendar	No deviation noted
24. Develop Appropriate Awareness and Training Content, Materials, and Methods	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	SOC 2 Report - Policy extract Sample Employee training calendar	No deviation noted
25. Implement the Training	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	SOC 2 Report - Policy extract Sample Employee training calendar	No deviation noted
26. Implement Security Reminders	Cisco has training practices that involve training as part of the new joining formalities and annually, thereafter.	Internal Portal covering security topics	No deviation noted
27. Monitor and Evaluate Training Plan	Trainings are conducted as part of the new joining formalities and annually.	HIPAA Training Presentation	No deviation noted

6. Security Incident Procedures (§ 164.308(a)(6))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
28. Determine Goals of Incident Response	Cisco has documented maximum tolerable period of disruption (MTPOD) and RTO for each category of assets.	MTPOD and RTO Values	No deviation noted
29. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism	Cisco has named key business function owners responsible for ensuring the continuity of the operations in the recently concluded BIA exercise.	Key executive names in the BIA	No deviation noted
30. Develop and Implement Procedures to Respond to and Report Security Incidents	DR test report for Campaign is in place. DR test report for Connect is in place. DR test report for Engage is in place.	DR Test report – Campaign DR Test report – Connect DR Test report – Engage	No deviation noted
31. Incorporate Post-Incident Analysis into Updates and Revisions	There has been no security incident reported in Cisco IT infrastructure that relates to data breach in the last one year.		No deviation noted

7. Contingency Plan (§ 164.308(a)(7))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
32. Develop Contingency Planning Policy	Cisco has shared a recently documented business impact analysis that shows the coverage of all systems, locations and resource dependencies including their risk.	Latest BIA/RA Report dated 30th Nov 2023	No deviation noted
33. Conduct an Applications and Data Criticality Analysis	Cisco has shared a recently documented business impact analysis that shows the coverage of all systems, locations and resource dependencies including their risk.	Latest BIA/RA Report dated 30th Nov 2023	No deviation noted
34. Identify Preventive Measures	AWS Controls - CISCO's three SAAS Solutions - Campaign, Connect and Engage - are hosted in separate independent Virtual Private Clouds (VPC) - There are separate networks for Production, pre-production, staging and Quality Assurance. - Each VPC implementation involves CISCO's chosen supporting infrastructure that includes EC2, and RDS. - Each VPC security involves a secure gateway, network access control at the subnets, and security groups at the individual instances. - RDS/Database connects allow inbound connection from private IP addresses. - Additional security involves AWS Shield (DDOS Protection), AWS GuardDuty (Threat detection and monitoring) and AlienVault (SIEM) as part of the overall security architecture.	AWS WAF Security Group	No deviation noted
35. Develop Recovery Strategy	DR test report for Campaign is in place. DR test report for Connect is in place. DR test report for Engage is in place.	DR Test report – Campaign DR Test report – Connect DR Test report – Engage	No deviation noted



36. Data Backup Plan and Disaster Recovery Plan Implementation Specifications (Both Required)	DR test report for Campaign is in place. DR test report for Connect is in place. DR test report for Engage is in place.	DR Test report – Campaign DR Test report – Connect DR Test report – Engage	No deviation noted
37. Develop and Implement an Emergency Mode Operation Plan	Cisco has shared a recently documented business impact analysis that shows the coverage of all systems, locations and resource dependencies including their risk.	Latest BIA/RA Report dated 30th Nov 2023	No deviation noted
38. Testing and Revision Procedure	DR test report for Campaign is in place. DR test report for Connect is in place. DR test report for Engage is in place.	DR Test report – Campaign DR Test report – Connect DR Test report – Engage	No deviation noted

8. Evaluation (§ 164.308(a)(8))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
39. Determine Whether Internal or External Evaluation Is Most Appropriate	Cisco has a combination of internal and external assessments in place. - Internal assessment involves internal audits - which are party of the iso 27001 internal audit. - External assessments are need-based. Apart from the above Cisco maintains a risk register that tracks ongoing security issues and vulnerabilities	Internal Audit Report	No deviation noted
40. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	- Cisco has an ongoing security measurement program that tests the security control effectiveness every month. -Any risk identified is managed through a central risk management program. - Additionally, CISCO is ISO 27001 certified for the same set of applications.	Internal Audit Report	No deviation noted
41. Conduct Evaluation	- Cisco has an ongoing security measurement program that tests the security control effectiveness every month. -Any risk identified is managed through a central risk management program. - Additionally, CISCO is ISO 27001 certified for the same set of applications. - Any deviation from the above is treated and brought to a logical closure as approved by the management.	Internal Audit Report	No deviation noted
42. Document Results	- Cisco has an ongoing security measurement program that tests the security control effectiveness every month. -Any risk identified is managed through a central risk management program. - Additionally, CISCO is ISO 27001 certified for the same set of applications. - Any deviation from the above is treated and brought to a logical closure as approved by the	Internal Audit Report	No deviation noted



	management. - Records are maintained in the central risk register.		
43. Repeat Evaluations Periodically	- Cisco has an ongoing security measurement program that tests the security control effectiveness every month. -Any risk identified is managed through a central risk management program. - Additionally, CISCO is ISO 27001 certified for the same set of applications. - Any deviation from the above is treated and brought to a logical closure as approved by the management. - Records are maintained in the central risk register. - Cisco Security team maintains an annual calendar of events that has monthly and annual review tasks associated with security evaluations.	Internal Audit Report	No deviation noted



9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
44. Identify Entities that Are Business Associates under the HIPAA Security Rule	There is no external Business Associate who have access to ePHI information, therefore this is Not Applicable		Not Applicable
45. Written Contract or Other Arrangement	There is no external Business Associate who have access to ePHI information, therefore this is Not Applicable		Not Applicable
46. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met	There is no external Business Associate who have access to ePHI information, therefore this is Not Applicable		Not Applicable
47. Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate	There is no external Business Associate who have access to ePHI information, therefore this is Not Applicable		Not Applicable

Physical Safeguards

10. Facility Access Controls (§ 164.310(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
48. Conduct an Analysis of Existing Physical Security Vulnerabilities	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable
49. Identify Corrective Measures	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable
50. Develop a Facility Security Plan	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable
51. Develop Access Control and Validation Procedures	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable
52. Establish Contingency Operations Procedures	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable
53. Maintain Maintenance Records	CISCO infrastructure is hosted with the cloud service providers (AWS and Azure), who provide the physical security infrastructure.		Not Applicable

11. Workstation Use (§ 164.310(b))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
54. Identify Workstation Types and Functions or Uses	CISCO has documented trusted device policy in place that defines the security requirements.	Trusted Device Standard	No deviation noted
55. Identify Expected Performance of Each Type of Workstation	CISCO has documented trusted device policy in place that defines the security requirements.	Trusted Device Standard	No deviation noted
56. Analyze Physical Surroundings for Physical Attributes	CISCO has a documented acceptable use policy for all employees.	Acceptable Use Policy	No deviation noted

12. Workstation Security (§ 164.310(c))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
57. Identify All Methods of Physical Access to Workstations	CISCO has a documented trusted device policy in place that defines the security requirements. CISCO has a documented acceptable use policy for all employees.	Trusted Device Standard Acceptable Use Policy	No deviation noted
58. Analyze the Risk Associated with Each Type of Access	CISCO has a documented trusted device policy in place that defines the security requirements. CISCO has a documented acceptable use policy for all employees.	Trusted Device Standard Acceptable Use Policy	No deviation noted
59. Identify and Implement Physical Safeguards for Workstations	CISCO has a documented trusted device policy in place that defines the security requirements. CISCO has a documented acceptable use policy for all employees.	Trusted Device Standard Acceptable Use Policy	No deviation noted

13. Device and Media Controls (§ 164.310(d)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
60. Implement Methods for Final Disposal of EPHI	- Cisco has a data retention policy for 90 days. - This is implemented through auto-configuration on the databases.	Retention Policy configuration	No deviation noted
61. Develop and Implement Procedures for Reuse of Electronic Media	Cisco has a Trusted Device Standard - that is applied for all end user devices.	Trusted Device Standard	No deviation noted
62. Maintain Accountability for Hardware and Electronic Media	Cisco has a Trusted Device Standard - that is applied for all end user devices.	Trusted Device Standard	No deviation noted
63. Develop Data Backup and Storage Procedures	Backup Policy	Backup Policy and settings	No deviation noted

Technical Safeguards

14. Access Control (§ 164.312(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
64. Analyze Workloads and Operations To Identify the Access Needs of All Users	CISCO has a documented access control policy. New employees/Users are provided access to the systems as part of standard HR employment formalities. Any privilege access is subject to approval by work supervisor. Temporary access is subject to automated or manual revocation procedure. All access to IT infrastructure is subject to an independent reporting. As part of separation policies, an employee's access is revoked.	Access Control Policy	No deviation noted
65. Identify Technical Access Control Capabilities	- The three products (Campaign/Connect and Engage) have role-based access features that customers can use. - Customers can choose between a native MFA feature or use their IAM solutions to integrate which results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination of on-prem Active directory and on-cloud IAM. - All user access is based on an access control policy where user identity is verified before provisioning access. - All privileged access is subject to an additional layer of supervisor approval. - All users have unique Identities	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted



66. Ensure that All System Users Have Been Assigned a Unique Identifier	- The three products (Campaign/Connect and Engage) have role-based access features that customers can use. - Customers can choose between a native MFA feature or use their IAM solutions to integrate which results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination of on-prem Active directory and on-cloud IAM. - All user access is based on an access control policy where user identity is verified before provisioning access. - All privileged access is subject to an additional layer of supervisor approval. - All users have unique Identities	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
67. Develop Access Control Policy	CISCO has a documented access control policy. New employees/Users are provided access to the systems as part of standard HR employment formalities. Any privilege access is subject to approval by work supervisor. Temporary access is subject to automated or manual revocation procedure. All access to IT infrastructure is subject to an independent reporting. As part of separation policies, an employee's access is revoked.	Access Control Policy	No deviation noted
68. Implement Access Control Procedures Using Selected Hardware and Software	- The three products (Campaign/Connect and Engage) have role-based access features that customers can use. - Customers can choose between a native MFA feature or use their IAM solutions to integrate which results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination of on-prem Active directory and on-cloud IAM. - All user access is based on an access control policy where user	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted

	identity is verified before provisioning access. - All privileged access is subject to an additional layer of supervisor approval. - All users have unique identities		
69. Review and Update User Access	Internal User access review is performed every six months.	Access Review Report	No deviation noted
70. Establish an Emergency Access Procedure	Access to the IT infrastructure supporting Cisco products and services ensures has no single user for any role. Access given to more than one individual ensures there is no single point of failure in case of an emergency.	Access Control Policy	No deviation noted
71. Automatic Logoff and Encryption and Decryption Implementation Specifications (Both Addressable)	- The three products (Campaign, Connect and Engage) have role-based access features that customer can use. - Customer can chose between a native MFA feature or use their IAM solutions to integrate that results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination on-prem Active directory and on cloud IAM. - All user access is based on access control policy where user identity is verified before provisioning access. - All privilege access is subject to an additional layer of supervisor approval. - Systems that connect via public internet has session time out implementation.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
72. Terminate Access if it is No Longer Required	Employee relieving process ensures access termination.	Relieving record	No deviation noted

15. Audit Controls (§ 164.312(b))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
73. Determine the Activities that Will Be Tracked or Audited	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
74. Select the Tools that Will Be Deployed for Auditing and System Activity Reviews	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
75. Develop and Deploy the Information System Activity Review/Audit Policy	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
76. Develop Appropriate Standard Operating Procedures	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies address security as part of the platform and the underlying infrastructure. These policies are subject to annual review.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
77. Implement the Audit/System Activity Review Process	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted

16. Integrity (§ 164.312(c)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
78. Identify All Users Who Have Been Authorized to Access EPHI	Access to systems is driven by access control policy. Users get access to systems based on their roles.	Access Tickets	No deviation noted
79. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
80. Develop the Integrity Policy and Requirements	- CISCO has a policy on secure software development lifecycle, where it assesses every change and release for security before deployment. - Both data in rest and data in motion are encrypted. - CISCO uses SonarQube (DAST) for scanning and identifying new vulnerabilities as part of the release process.	SDLC Policy SonarQube Report	No deviation noted
81. Implement Procedures to Address These Requirements	- CISCO has a policy on secure software development lifecycle, where it assesses every change and release for security before deployment. - Both data in rest and data in motion are encrypted. - CISCO uses SonarQube (DAST) for scanning and identifying new vulnerabilities as part of the release process.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted



82. Implement a Mechanism to Authenticate EPHI	- CISCO has a policy on secure software development lifecycle, where it assesses every change and release for security before deployment. - Both data in rest and data in motion are encrypted. - CISCO uses SonarQube (DAST) for scanning and identifying new vulnerabilities as part of the release process.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
83. Establish a Monitoring Process To Assess How the Implemented Process Is Working	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	AlienVault Report	No deviation noted

17. Person or Entity Authentication (§ 164.312(d))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
84. Determine Authentication Applicability to Current Systems/Applications	- The three products (Campaign, Connect and Engage) have role-based access features that customer can use. - Customer can chose between a native MFA feature or use their IAM solutions to integrate that results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination on-prem Active directory and on cloud IAM. - All user access is based on access control policy where user identity is verified before provisioning access. - All privilege access is subject to an additional layer of supervisor approval. - Systems that connect via public internet has session time out implementation.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
85. Evaluate Authentication Options Available	- The three products (Campaign/Connect and Engage) have role-based access features that customer can use. - Customer can chose between a native MFA feature or use their IAM solutions to integrate those results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination on prem Active directory and on cloud IAM. - All user access is based on access control policy where user identity is verified before provisioning access. - All privilege access is subject to an additional layer of supervisor approval.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted



86. Select and Implement Authentication Option	- The three products (Campaign/Connect and Engage) have role-based access features that customer can use. - Customer can chose between a native MFA feature or use their IAM solutions to integrate those results in user identification and authentication. - For Cloud access, Cisco has implemented MFA using a combination on prem Active directory and on cloud IAM. - All user access is based on access control policy where user identity is verified before provisioning access. - All privilege access is subject to an additional layer of supervisor approval.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
--	--	---	--------------------

18. Transmission Security (§ 164.312(e)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
87. Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information	- Cisco has implemented Security Event Information Management (SIEM) - AlienVault - managed by third party. - All events and breach indicators are reported by the managed provider to contact points in CISCO for further remediation.	SIEM Report	No deviation noted
88. Develop and Implement Transmission Security Policy and Procedures	Cisco has implemented transmission security on all three platforms by implementing TLS 1.2 or above.	TLS Evidences on three products	No deviation noted
89. Implement Integrity Controls	- CISCO has a policy on secure software development lifecycle, where it assesses every change and release for security before deployment. - CISCO uses SonarQube (DAST) for scanning and identifying new vulnerabilities as part of the release process.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
90. Implement Encryption	Cisco has implemented encryption at various layers. - Application-level encryption using Java encryption class/libraries - CSP provisioned services like AWS Key management and Azure Key Vault - Cisco has implemented transmission security on all three platforms by implementing HTTPS/TLS 1.2 or above. - Additional security by database encryption settings	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted

Organizational Requirements

19. Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
91. Contract Must Provide that Business Associates Adequately Protect EPHI	There are no business associates that process ePHI on behalf of CISCO.		Not Applicable
92. Contract Must Provide that Business Associate's Agents Adequately Protect EPHI	There are no business associates that process ePHI on behalf of CISCO.		Not Applicable
93. Contract Must Provide that Business Associates will Report Security Incidents	There are no business associates that process ePHI on behalf of CISCO.		Not Applicable
94. Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached	There are no business associates that process ePHI on behalf of CISCO.		Not Applicable
95. Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements	There are no government entities/business associates that process ePHI on behalf of CISCO.		Not Applicable
96. Other Arrangements for Covered Entities and Business Associates	There are no business associates that process ePHI on behalf of CISCO.		Not Applicable

20. Requirements for Group Health Plans (§ 164.314(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
97. Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of EPHI	Cisco is not a group health plan		Not Applicable
98. Amend Plan Documents of Group Health Plan to Address Adequate Separation	Cisco is not a group health plan		Not Applicable
99. Amend Plan Documents of Group Health Plan to Address Security of EPHI Supplied to Plan Sponsors' Agents and Subcontractors	Cisco is not a group health plan		Not Applicable
100. Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents	Cisco is not a group health plan		Not Applicable

Policies and Procedures and Documentation Requirements

21. Policies and Procedures (§ 164.316(a))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
101. Create and Deploy Policies and Procedures	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies are subject to annual review, which is reflected in the document history	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted

22. Documentation (§ 164.316(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s Demonstrated	Auditor Opinion
102. Update Documentation of Policy and Procedures	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies are subject to annual review, which is reflected in the document's history	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted



103. Draft, Maintain and Update Required Documentation	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies are subject to annual review, which is reflected in the document history.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted
104. Retain Documentation for at Least Six Years	Documents are relevant records are retained for a period of six years.	Responsibility of the HIPAA Security Officer	No deviation noted
105. Assure that Documentation is Available to those Responsible for Implementation	Cisco has a corporate intranet where all policies and procedures related to HIPAA are published and are visible to all staff.	Intranet	No deviation noted
106. Update Documentation as Required	CISCO has documented policy for each of the three products - Connect, Engage and Connect - Cisco has provided documentation supporting its security. These policies are subject to annual review, which is reflected in the document history.	CISCO Campaign - Security Overview CISCO Engage - Security Overview CISCO Connect - Security Overview CISCO Secure Development Lifecycle Policy	No deviation noted