NUANCE HEALTHCARE

SOC 2 TYPE 2 REPORT - SECURITY, AVAILABILITY, AND CONFIDENTIALITY

INDEPENDENT SERVICE AUDITORS' REPORT ON CONTROLS PLACED IN OPERATION FOR HOSTED INFRASTRUCTURE SERVICES FOR THE PERIOD MAY 1, 2017 THROUGH APRIL 30, 2018

NUANCE HEALTHCARE

CONTROLS PLACED IN OPERATION FOR HOSTED INFRASTRUCTURE SERVICES
FOR THE PERIOD MAY 1, 2017 THROUGH APRIL 30, 2018

CBM
CENTERED ON YOUR SUCCESS

7910 WOODMONT AVENUE
SUITE 500
BETHESDA, MD 20814
(T) 301.986.0600
(F) 301.986.0432

2100 PENNSYLVANIA AVENUE, NW
SUITE 580
WASHINGTON, DC 20037
(T) 202.822.0717

Independent Service Auditors' Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

To Nuance Healthcare:

Scope

We have examined Nuance Healthcare's accompanying description of its Hosted Infrastructure Services system for Dragon Medical 360 Direct throughout the period May 1, 2017 through April 30, 2018, (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period May 1, 2017 through April 30, 2018, to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100A*, 2016 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (applicable trust services criteria).

As indicated in the description, Nuance Healthcare uses two subservice organizations for data center hosting of the audited application. The description includes the controls of Nuance Healthcare and excludes controls of the subservice organization. The description also indicates that certain trust services criteria can only be met if the subservice organization's controls, contemplated in the design of Nuance Healthcare's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to the controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Nuance Healthcare's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section I of this report, Nuance Healthcare has provided its assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Nuance Healthcare is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period May 1, 2017 through April 30, 2018. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves the following:

- performing procedures to obtain evidence about the fairness of presentation of the description based on the description criteria, and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section III of this report.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria—

a. the description fairly presents the Hosted Infrastructure system that was designed and implemented throughout the period May 1, 2017 through April 30, 2018.

Opinion (Continued)

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period May 1, 2017 through April 30, 2018, and the subservice organization and user entities applied the controls contemplated in the design of Nuance Healthcare's controls throughout the period May 1, 2017 through April 30, 2018.

c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period May 1, 2017 through April 30, 2018, if the subservice organization and user entity controls contemplated in the design of Nuance Healthcare's controls operated effectively throughout the period May 1, 2017 through April 30, 2018.

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Nuance Healthcare; user entities of Nuance Healthcare's Hosted Infrastructure system during some or all of the period May 1, 2017 through April 30, 2018, 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, and other parties.
- Internal control and its limitations.
- User entity responsibilities, complementary user entity controls, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Councilor, Buchanan + Mitchell, P.C.

Bethesda, Maryland
September 6, 2018

Councilor, Buchanan & Mitchell, P.C.

SECTION I: ASSERTION OF NUANCE COMMUNICATIONS, INC.

We have prepared the accompanying description of Nuance Healthcare's (Nuance's) Hosted Infrastructure Services system ("description") for Dragon Medical 360 Direct for the period May 1, 2017 through April 30, 2018, based on the criteria in items (I)(A)-(B) below, which are the criteria for a description of a service organization's system in paragraphs 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2®) (description criteria). The description is intended to provide users with information about the Hosted Infrastructure Services system that may be useful when assessing the risks arising from interactions with Nuance Healthcare's Hosted Infrastructure Services system, particularly information about the suitability of design and operating effectiveness of Nuance Healthcare's controls to meet the criteria related to security, availability, and confidentiality set forth in TSP section 100A, *2016 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Service Criteria*) (applicable trust services criteria).

Nuance Healthcare uses a subservice organization to provide data center hosting services. The description includes only the controls of Nuance Healthcare and excludes controls of the subservice organization. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization's controls contemplated in the design of Nuance Healthcare's controls are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the subservice organization.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Nuance Healthcare's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

I. The description fairly presents the Hosted Infrastructure Services for the specified product as of May 1, 2017 through April 30, 2018, based on the following description criteria:

   A. The description contains the following information:

      1. The types of services provided;

      2. The components of the system used to provide the services, which are as follows:

         a. *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

         b. *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

         c. *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         d. *Processes.* The automated and manual processes.

         e. *Data.* Transaction streams, files, databases, tables, and output used or processed by the system;

SECTION I: ASSERTION OF NUANCE COMMUNICATIONS, INC. (CONTINUED)

3. The boundaries or aspects of the system covered by the description;
4. How the system captures and addresses significant events and actions;
5. For information provided to, or received from, subservice organizations or other parties:
    a. how such information is provided or received and the role of the subservice organization and other parties;
    b. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;
6. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
    a. Complementary user entity controls contemplated in the design of the service organizations system;
7. With regard to the subservice organization using the carve-out method:
    a. the nature of the services provided by the subservice organization;
    b. each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
8. Other aspects of Nuance Healthcare's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable security, availability, and confidentiality criteria;

B. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs;

II. The controls stated in the description were suitably designed and operated effectively throughout the period May 1, 2017 through April 30, 2018, to meet the applicable trust services criteria.

The examination was limited to the hosting of a selected set of product services by Nuance Healthcare. Accordingly, the examination did not extend to any activities or procedures using client devices or in effect at client premises. It is each client auditor's responsibility to evaluate this information in relation to a client entity's internal controls in place in order to obtain an understanding of the internal controls and assess control risk. The portions of the internal controls provided by the client entities' and Nuance Healthcare must be evaluated together. If effective client internal controls are not in place, Nuance Healthcare's controls may not compensate for such weaknesses.

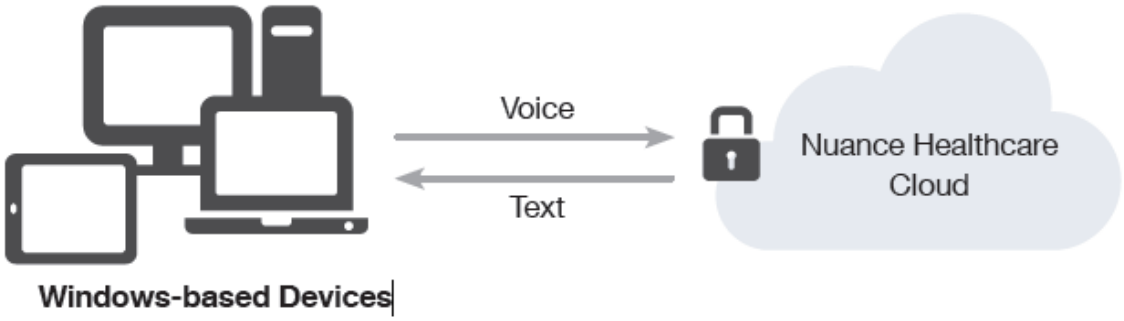
SECTION II: DESCRIPTION OF THE SYSTEM

Description of the Systems Provided by Nuance Healthcare

Nuance Communications, Inc., is a leading provider of voice and language solutions for businesses and consumers around the world. Nuance Healthcare leads the market in creating clinical understanding solutions that drive smart, efficient decisions across healthcare. More than 500,000 physicians and 10,000 healthcare facilities worldwide leverage Nuance Healthcare's award-winning, voice-enabled clinical documentation and analytics solutions to support the physician in any clinical workflow and on any device.

Description of Dragon Medical 360 Direct Services

Dragon Medical 360 Direct, based on technology acquired from Phillips Speech Division in 2008, is a secure, cloud-based speech recognition solution that allows clinicians to document the complete patient story using voice while allowing healthcare organizations to easily deploy medical speech recognition across their enterprise.



Highly scalable and ready-to-use, Dragon Medical 360 Direct provides cloud-based clinical speech recognition across an existing infrastructure of Windows-based devices, including virtualized and remote-access PCs. The lightweight Windows client application downloads and installs in minutes and provides a secure connection to the Nuance cloud. It delivers cross-channel access to user voice profiles, real-time speech-to-text and the latest medical dictionary, terms, phrases, and clinical formatting rules to ensure a fast and accurate speech recognition experience. Additional features include specialty-specific medical language models, automated user accent detection and gain control, custom vocabularies and templates, and voice-based correction.

Dragon Medical 360 Direct can be installed on any clinical workstation or laptop in just minutes without the need for complex configurations. Once installed, clinicians simply open the application from the Windows Start menu, place the cursor where they want speech-recognized text to appear, and start dictating into any clinical, or non-clinical, Windows-based application (e.g., EHR, Microsoft Outlook, and Microsoft Word). Standard preferred dictation hardware, such as the PowerMic II, is plug-and-play, but other hardware is also supported. Zero voice profile training, automatic accent detection, and profiles that continue to adapt and improve over time, ensure an optimal clinician experience from the start.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Components of the Dragon Medical 360 Direct System

Infrastructure and Software

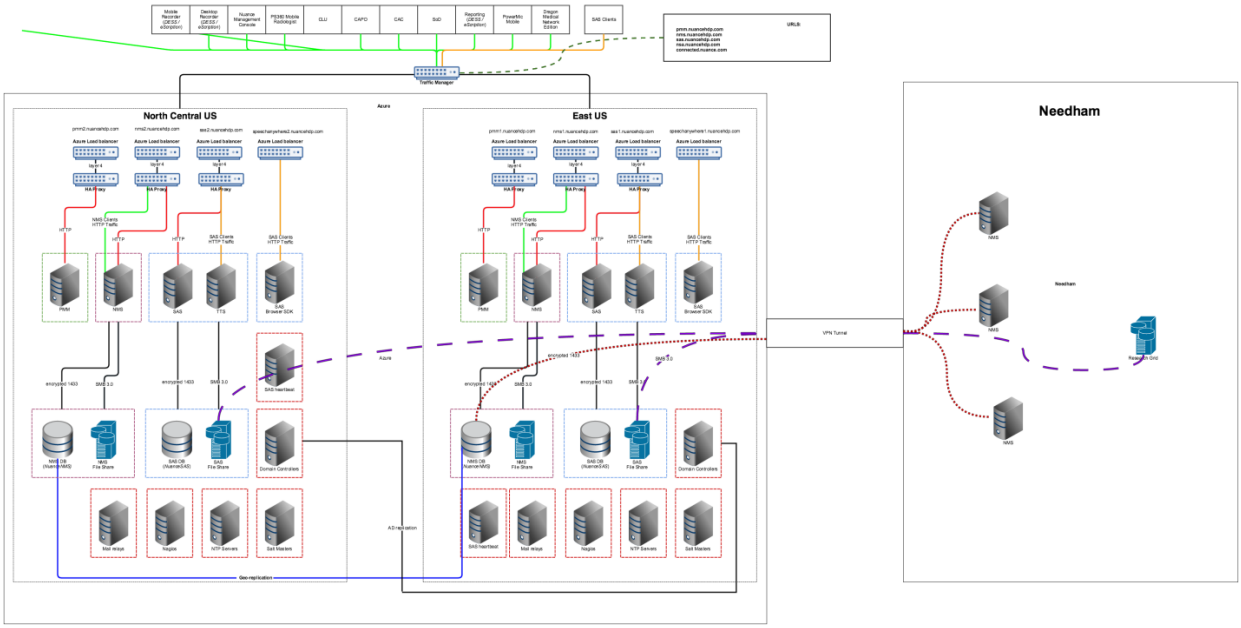
Dragon Medical 360 Direct is supported by active-active instances at two Microsoft Azure cloud computing data centers providing highly scalable, responsive, and available environments. Customer transactions are dispatched to one of two data centers by Azure traffic management, and traffic loads are balanced across components within each center. The virtualized environments are mirrored at each site and include:

- Web interfaces to the hosted services, virtualized clustered Windows Server 2012 R2 configurations running primarily C# and .NET code;
- Speech Anywhere Services (SAS) nodes, virtualized servers running proprietary C code that perform speech to text conversion;
- PowerMic Mobile (PMM) servers, virtualized Windows servers with C# application code, supporting acquisition of audio from PowerMic devices;
- Data services, provided by clustered Azure provisioned MS SQL Server databases;
- Nuance Management Server (NMS) servers, used for license validation, auto-text command processing, and other services. (Transactions are license based and not user based, although users are customer defined and assigned licenses.);
- Administrative servers supporting: Active Directory (AD), monitoring, time services (NTP), configuration management (Salt), eMail, deployment (Jump), general management, e.g. SQL Studio;
- Network security protection leveraging Trend Micro Intrusion Prevention System (IPS) and Intrusion Detection System (IDS);
- Environments for: Production, Development, Staging, and QA.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Infrastructure and Software (Continued)

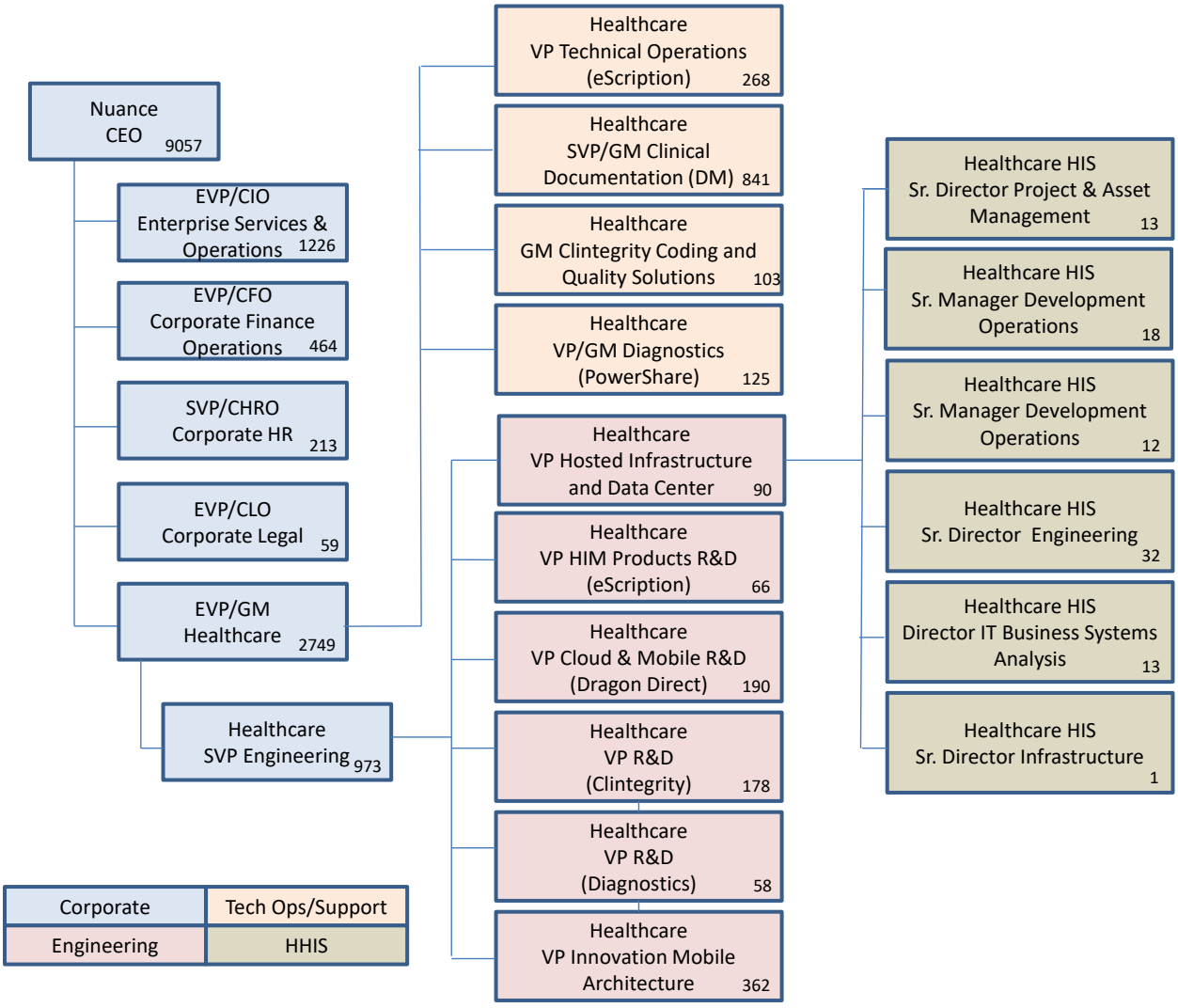
Captured audio is submitted from the customer application interface via authorized encrypted connections, converted to text, and returned to the customer application.



SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

People

Nuance Healthcare is organized into functional areas as depicted in the following diagram and described below. Nuance Healthcare (2,600 staff) is a business segment of the larger Nuance Communications, Inc. Segments of the Nuance Healthcare organization relevant to the current audit are shown below (number of staff in the lower right corner).



- Corporate - Executives, senior operations staff, and company administrative support, such as legal, training, contracting, accounting, finance, and human resources.

Within the Healthcare segment two major groups are relevant for this audit.

- Technical Operations/Support - Staff in this area provides for operational implementation, operation, and support across all of the application products.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

People (Continued)

- Technical Operations
  - Product liaison and client executives
  - Customer service center staff supports each product taking customer phone calls, responding to emails, and handling various interactions related to product use, performance, issues, etc.
- Professional Services
  - Creates application configurations for new customers to be instantiated in the production environment by HHIS Development Operations
- Nuance Transcription Services (NTS)
  - A large organization of Nuance Healthcare managed Medical Transcriptionists (MTs) supporting review and update of eScription generated text

- Engineering
  - Staff developing and supporting Healthcare application products
  - Hosted Infrastructure and Data Center Group, also known as Healthcare Hosted Infrastructure Services (HHIS), implements and supports operation of application environments
    - Project and Asset Management
      - Project Management
      - Business Operations Support
      - Budget/Forecasts
      - Vendor Management
      - Change Management
      - Access Management
      - Quality Assurance
      - Compliance
      - Governance

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

People (Continued)

- Acquisition
- Integration
- Asset Management Program
- Operations and Process Improvement
  - Metrics and KPI's
  - Service Assurance Management
  - Rapid Systems Provisioning and Deployment
  - Tools and Automation

♦ Development Operations (two groups)

- Product Relationship Management
- Deployment -- Dev to Ops End to End Delivery
- Full Stack Systems Development Life Cycle (SDLC) Support
- Systems, Storage, Network Support for Application Implementation
- Liaison for OS & Above (Middleware and Applications)
- Azure Environment
- Cloud Architecture
- Patching/Change Support
- Tier 2 Support

♦ IT Business Systems Analysis

- Service Reliability Center (SRC) / Network Operations Center (NOC) providing 24/7 real time monitoring and event coverage via Melbourne and India sites
- Incident Management
- Reason for Outage (RFO) Analysis
- Expansion of Ops Services (e.g. Telco and Network)

♦ Hosted Infrastructure Engineering

- Database Administration

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

People (Continued)

- Servers/Server Virtualization
- Storage
- Network/Telco
- Infrastructure Services
  - Active Directory
  - Authentication Services
  - Certificate Management
  - Antivirus
  - Security Infrastructure
  - NTP
  - DNS
  - DHCP
  - Monitoring Infrastructure
  - Load Balancing
  - Terminal Services
  - Telecom
- Patching/Change Support
- Tier 1, 2, and 3 Support
- Data Center Operations
  - Contract Management
  - Expense Analysis
  - Capacity Planning
  - Layer 1 Standards
  - Break/Fix Support
  - Rack and Stack
- Monitoring Architecture
  - Dashboards
  - Tool Integration
  - Log Management

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Processes

Processes have been defined and implemented to cover the following key security life cycle areas:

- Personnel hiring, training, and compliance processes
- Performance of annual and ongoing security risk assessments and implementation of associated mitigations
- Authentication/authorization, changes to, and termination of information system access
- Physical security
- Change management process
- Vulnerability and patch management process
- Critical incident management process
- Asset management processes
- Security and system operation monitoring

These processes are described in more detail in the control environment section of this document.

Data

The following data categories are associated with the Dragon Medical 360 Direct product. Nuance Healthcare applications are source systems that may, or may not, feed into Customers' Electronic Health Records. Thus Nuance is subject to HIPAA as a Business Associate of its customers. While much audio and associated text data is retained, it is only used to refine the speech-to-text or other analytic models. Data flows are described in the product architecture and infrastructure overview sections.

- Customer Information - user account, licensing, configuration information - stored in a NMS MS SQL Server database
- Speech profiles - stored in a MS SQL Server database
- Persisted audio and text files, including PHI, stored in a file system
- Server images
- Server configuration information
- Code base (includes vendor software/firmware, associated licenses, and developed application product code)

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

System Boundaries

This audit is scoped to Nuance Healthcare hosted services in support of the Dragon Medical 360 Direct product, and specifically those services that are hosted in United States facilities.

Control Environment

The control environment provides the overall context for all aspects of internal control. Factors such as the organizational structure, ethical values, assignment of authority and responsibility, and management oversight drive effective adoption and execution of control measures.

Organizational Structure, Authority, and Responsibility

An entity's organizational structure provides a framework within which its objectives are planned, executed, controlled, and monitored. Significant aspects of establishing an effective organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Nuance executive management has ultimate responsibility for defining these areas of authority and responsibility and for establishing reporting relationships and authorization protocols. The executive and organizational structure, lines of authority, reporting, and responsibility were summarized above.

Nuance is also guided by a ten member Board of Directors and a Governance Committee that ensures the Company has and follows appropriate governance standards.

Integrity and Ethical Values

The effectiveness of controls is based on the integrity and ethical values of the people who create, administer, and monitor them. The Board of Directors of Nuance Communications, Inc., adopted a Code of Business Conduct and Ethics for its directors, officers and employees. All employees are required to read and understand this Code, sign-off on agreement with code upon hire, uphold these standards in day-to-day activities, and comply with all applicable policies and procedures. The code is intended to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- Avoidance of conflicts of interest, including disclosure to an appropriate person or persons identified in this Code of any transaction or relationship that reasonably could be expected to give rise to such a conflict;
- Full, fair, accurate, timely, and understandable disclosure in reports and documents that the Company files with, or submits to, the United States Securities and Exchange Commission (the "SEC") and in other public communications made by the Company;
- Compliance with applicable governmental laws, rules and regulations;

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Integrity and Ethical Values (Continued)

- Adherence to all Nuance policies, including but not limited to Foreign Corrupt Trade Practices and Insider Trading policies;
- The prompt internal reporting to an appropriate person or persons identified in this Code of violations of this Code; and
- Accountability for adherence to this Code.

Security Organization and Management

Nuance has defined an Information Security Policy that provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. The Nuance Security Organization (NSO) develops and maintains Information Security Policy and publishes it to all internal employees and to external parties given a business need.

Nuance has a dedicated security team responsible for managing information security and privacy providing for annual security and privacy awareness training, assessment and mitigation of threats, monitoring and addressing of vulnerabilities, and monitoring overall change for security impact. The security team has put in place an extensive set of policies and procedures, as documented in:

- POL - Global Security Framework 1.6-FINAL.PDF
- Nuance Healthcare Privacy Policies v 1 3.pdf
- Nuance Healthcare Division Security Policies and Procedures 11-2017 FINAL.PDF

As well as general security policy and organization, the documents cover key security areas:

- Asset Management
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Personnel Security

Nuance hiring practices are formalized and performed via a detailed job requisition process. Employees are hired in accord with job descriptions specifying requisite education and experience levels. Background checks are required for all new hires. As noted above, employees are required to read and agree to the Nuance code of conduct. All employees are required to attend annual security, privacy and compliance awareness training covering a number of areas, including procedures and requirements to report security and privacy issues and incidents. Management monitors training compliance. Defined sanctions and processes are in place to address violations of the code of conduct.

Physical Security (Critical Availability Item)

Physical security policies, processes, and mechanisms are in place at Microsoft Azure facilities and are stringently enforced at the two SOC 2 Type 2 certified data centers hosting the Dragon Medical 360 Direct application. The facilities are highly secure with a robust physical environment designed to provide highly available computing infrastructure. The data centers are in compliance with the following requirements:

- Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors.
- Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.
- Physical access to the data center is reviewed quarterly and verified by the data center operations team.
- Physical access mechanisms (e.g. access card readers, biometric devices, man traps, portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
- The data center facility is monitored 24/7 by security personnel.
- Environmental controls have been implemented to protect systems inside the facility, including temperature and HVAC controls, fire detection and suppression systems, and power management systems.

System Account and Access Management

The HHIS Access Provisioning Process is a formal process for establishing and limiting staff access to Nuance Healthcare HHIS systems. Employees are granted logical and physical access to in-scope systems based on system documented requests that are reviewed and approved by appropriate management personnel.

In accord with the HHIS Access Termination Process, the human resources department provides HHIS with notification of employee termination. HHIS disables the associated user id and revokes the associated access privileges. The changes are documented in the request system.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

System Account and Access Management (Continued)

Initial guidelines for role based access control have been developed and are captured in the HHIS Role Based Access Control (RBAC) Guidelines document. RBAC will be implemented as is feasible and appropriate, but is dependent on the complex task of coordinating and defining consistent role definitions.

Administrative access to Active Directory, UNIX/Linux servers, VMware servers, databases, storage, and network devices is restricted to authorized employees and is managed with the HHIS Access Provisioning Process. Account sharing is not allowed, with the exception of some generic "root" type accounts whose use is minimized. User identities are audited quarterly.

Policies and mechanisms require unique user identification numbers, names, and passwords for authentication of all HHIS staff. Password constraints are as follows:

- Passwords have a minimum of 8 characters, including 2 non-alphanumeric characters.
- Passwords expire every 90 days for non-privileged accounts and 180 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.
- The last 10 passwords cannot be reused (5 passwords for privileged accounts).

Customer access control varies by product. For Dragon Medical 360 Direct, a set of customer administrators and their privileges is defined as part of the initial customer configuration by the Nuance Healthcare Provisioning Services group. That configuration is then implemented in production by HHIS Development Operations in accord with the HHIS Change Management Process. Dragon Medical 360 Direct is a transactional system, and service access is gated by customer licenses as validated by the Nuance Management Server (NMS). NMS provides a wide range of product configuration, security, and management options. Customer administrators are configured for NMS, and they utilize it to define organizations and users of various types, allocate licenses (both individual and organizational), establish speech processing options, backup, reporting, etc. When users are registered in the system they are associated with a license which enables their access to Dragon Medical 360 Direct services.

Change Management

Nuance Healthcare has formalized change management in place, as defined by the HHIS Change Management Process document. The process requires identification and recording of changes in the request tracking system, review and assessment of risk and potential impact of proposed changes, approval of proposed changes, testing of changes to verify operational functionality, and communication of change nature and status throughout the process. Proposed changes are evaluated to determine if they present a security or other operational risk and what mitigating actions, including employee and customer entity notifications, must be performed. All changes must have back out plans specified. The HHIS Change Advisory Board (CAB) management team meets weekly to review and schedule changes to the HHIS environments. Emergency changes follow the formal change

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Change Management (Continued)

management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented. Changes to infrastructure and software are developed and tested in separate development or test environments before implementation. Developers are not permitted to implement changes independently or alter production environments.

Vulnerability and Patch Management

The HHIS Vulnerability Management Process implements a formal structured process for monthly internal and external infrastructure scans to identify vulnerabilities at HHIS data centers. Regular monitoring of CERT alerts and HITRUST Monthly threat briefings is another source of vulnerability identification. Finally, vendor patch distributions provide a third input into the vulnerability management process. In all of these cases, owners of the impacted assets are identified, and the identified vulnerabilities are evaluated. The risk associated with vulnerability is ranked according to its impact including timelines for implementation, and a remediation plan is agreed in joint discussion with asset and product owners, data center staff, management, and the security team. Remediation is implemented and assessed following implementation. Vulnerabilities and their disposition are tracked by the Security Organization.

Nuance Healthcare uses standardized server build checklists and server policy management tools to help secure its servers, implementing only required services and thus reducing the scope of vulnerabilities. Antivirus software (Microsoft Security Essentials) has been installed and activated to detect and protect against malicious code.

Risk Assessment Management

In accord with defined Nuance Healthcare security policy, an extensive risk management capability has been implemented using the RSA Archer GRC (Governance, Risk, Compliance) Platform.

- https://www.rsa.com/en-us/products/governance-risk-and-compliance/archer-platform

The product provides an overall framework for corporate governance, enterprise risk management, and management of corporate compliance to regulatory mandates. The RSA Archer GRC Platform presents a unified, very flexible, and adaptable common foundation for managing policies, controls, risks, assessments, and deficiencies across an enterprise. The implementation will evolve and be adapted to new requirements and changes over time. The initial Nuance implementation utilizes the RSA Archer GRC IT Risk Management capability.

- https://www.rsa.com/content/dam/rsa/PDF/ds-rsa-archer-it-risk-management-h14804.pdf

Key features are:

- Centralized catalog of IT assets
- IT controls repository and taxonomy
- Pre-built risk and threat assessments
- Risk repository and taxonomy

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Risk Assessment Management (Continued)

- Ability to manage risk assessment processes
- Consolidated issues management process
- Consolidated list of findings from compliance and audit
- Consolidated list of remediation plans for compliance
- Managed exceptions with appropriate risk sign off

Risk assessments are conducted when a significant event or change occurs to the information system, organization or legal requirements, or at least once per year. Current annual system security risk assessments specifically assess general security and HIPAA requirements. As well as formal risk assessment activity, the information security team assesses security through ongoing review and analysis of security event logs, ongoing vulnerability assessments, periodic special penetration tests, and regular management meetings with HHIS personnel.

Incident Management

Nuance Healthcare has a formalized Critical Incident Management process in place. Customers or internal staff/functions can identify potential issues which are vetted against incident criteria defined by the Critical Incident Management Process, and if found to meet the criteria result in the Critical Incident Manager opening an incident. The Manager records the incident, reviews it with management and technical staff, and coordinates resolution actions which most likely result in the creation of change tickets. The Incident Manager is the responsible authority for coordinating communication, resolution actions and eventual closure.

System Monitoring (Critical Availability Item)

The HHIS infrastructure and HHIS Site Reliability Center (SRC) teams use a variety of utilities including Check_MK, Nagios, Idera SQL Diagnostic Manager, scanning tools, and native component monitoring capabilities to identify and detect possible operational anomalies and incidents. The information reported by these tools includes such items as loading and resource utilization, failover, ping response, and notifications of other exceptional system events. Alerts are reviewed by the Site Reliability Center staff and by security and system administration teams. Critical alerts result in the automatic creation of an incident ticket in the RemedyForce system. Upon review, they may be entered into the Critical Incident Management system.

Dragon Medical 360 Direct Key Performance Indicators (KPIs) are available for viewing continuously through an online dashboard. These metrics, including resource utilization and capacity indicators, are reviewed at monthly meetings by product development, development operations, operations and other key stake holders to identify issues and plan for increased or changing capacity needs. Resulting change requests drive system updates to support increased capacity or to address other issues.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

System Monitoring (Critical Availability Item) (Continued)

The Sumo Logic product has been implemented. It provides continuous data collection and log aggregation from all systems/applications. The aggregated data enables incident detection and provides rich sources for post incident analysis and recovery. The Sumo Logic dashboard is monitored by the Security Operations Center in India with management in Montreal, Canada, and accessibility by the security leadership team in Burlington, MA.

Data Back Up and Recovery (Critical Availability Item)

Dragon Medical 360 Direct is supported by active-active instances at two Microsoft Azure cloud computing data centers providing highly scalable, responsive, and available environments. Application critical data is held in NMS MS SQL Server databases. The NMS SQL databases are replicated three times in each data center, and are also geo-replicated to the alternate center. Only five seconds of data loss is expected for NMS SQL data if a failover is required. Speech Anywhere System (SAS) SQL databases and multiple file shares also containing data are replicated three times in each data center. The file shares are also replicated to a secondary file share which also has three replicas. SAS SQL data and file shares are not geo-replicated to the alternate data center as they do not contain critical data. A full backup of SQL database history is performed nightly, snapshots are taken hourly and transaction logs are saved every two minutes. Active Directory data is replicated and synched between the two centers. Access to all data including replicas and backups is restricted to authorized personnel.

Since the Azure sites and the Dragon Medical 360 Direct instances are both active, at any point in time, customers can be directed to an alternate center. In the case of interruption of full service at the primary site, the critical component requiring failover to the alternate is the NMS SQL database, and the only associated impacted functionality is voice-command processing. Dictation processing continues, depending on the version of the customer client, either after a retry or automatically, with minimal customer disruption.

The required actions to make an alternate center a full primary are to make the NMS SQL database at the operational site the primary and to update connection parameters. The NMS SQL database at the alternate site contains current data through the geo-replication process. All other data can be recreated dynamically, if necessary. Failover/failback and recovery scenarios have been successfully tested. Full failover can be completed within five minutes. Customer dictation support, except voice-command processing, is available during the failover operation. A plan is being developed to alternate, approximately at a six month interval, the primary and secondary data centers between the two Azure sites, ensuring both are current and fully operational.

Asset Management

Nuance Healthcare maintains a complete inventory of hardware assets across all HHIS facilities. The inventory is maintained in a Remedy database. Interim asset identification of software assets has been started. A road map has been prepared for the evolution of the Remedy based capabilities, eventually implementing a full Configuration Management database.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Information and Communication Systems

The Nuance policy documents cited above clearly define information security and privacy policies to help ensure that employees understand their individual roles and responsibilities concerning security processing and controls. Employees are required to attend annual security awareness training that refreshes and updates their security skills.

Nuance Healthcare maintains internal SharePoint and Confluence sites that are populated with detailed application, architecture and system information and processes providing employees with ready access to information on application system functions, implementation, and operation. Nuance The Voice site contains general corporate information.

Ticketing systems provide a record and notification basis of changes, Customer Service Center recorded issues, and incidents.

Internal email is also used to communicate time-sensitive information regarding security and system availability, notifying key personnel in the event of problems. External emails are used to inform customers of issues, changes, and updates to product functionality.

Monitoring of the Subservice Organization

Data center space, power, communications connections, HVAC, and physical security services for the Dragon Medical 360 Direct application are provided by:

- Microsoft Azure North America East Central U.S. - Ashburn, VA
- Microsoft Azure North America North Central U.S. - Chicago, IL

Although controls relating to physical security and implemented by the data center facilities are included in the overall Healthcare control environment specification, these and other services summarized above as provided by the data center vendors will be treated as carve-out services.

Management of Nuance Healthcare receives and reviews the Type 2 SOC 2 report of the subservice organizations on an annual basis. In addition, through its daily operational activities, management of Nuance Healthcare monitors the services performed by Microsoft Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to subservice organization management.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Complementary Subservice Organization Controls

Nuance Healthcare's controls related to the Hosted Infrastructure system cover only a portion of the overall internal control for each user entity of Nuance Healthcare. It is not feasible for the control objectives related to Hosted Infrastructure to be achieved solely by Nuance Healthcare. Therefore, each user entities controls must be evaluated in conjunction with Nuance Healthcare's controls and the related tests and results described in Section III of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below:

- The subservice organization is responsible for maintaining logical security over the servers and other hardware devices upon which the Dragon Medical 360 Direct application is hosted.
- The subservice organization is responsible for notifying Nuance Healthcare of any security incidents related to security over the servers and other hardware devices upon which the Dragon Medical 360 Direct application is hosted.
- The subservice organization is responsible for maintaining physical security over its data center in which the servers used to host the Dragon Medical 360 Direct application are housed.

User Entity Responsibilities

The following list includes controls that Nuance Healthcare assumes its user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

- Customers are responsible for managing compliance with applicable laws/regulations.
- Customers are responsible for ensuring that their users are establishing appropriate controls over the use of their Nuance Healthcare accounts and passwords.
- Customers are responsible for disabling/deleting account access to their Nuance Healthcare services upon employee role change/employee termination.
- Customers are responsible for ensuring that their users following appropriate security practices while using Nuance Healthcare applications.
- Customers' administrators are responsible for selection and use of their passwords.
- Customers are responsible for ensuring the confidentiality of user IDs and passwords use to access Nuance Healthcare applications.

Entity Controls Testing Spreadsheet

The examination was limited to operation of Dragon Medical 360 Direct services by Nuance Healthcare HIS. Accordingly, the examination did not extend to any activities or procedures using client devices or in effect at client premises. It is each client auditor's responsibility to evaluate this information in relation to a client entity's internal controls in place in order to obtain an understanding of the internal controls and assess control risk. The portions of the internal controls provided by the client entities and Nuance

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Entity Controls Testing Spreadsheet (Continued)

Healthcare HIS must be evaluated together. If effective client internal controls are not in place, Nuance Healthcare's HIS controls may not compensate for such weaknesses.

The controls presented and examined address the security, availability, and confidentiality trust principles.

Significant Changes during the Review Period

None.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC1.0	**Common Criteria Related to Organization and Management**			
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	A functional organizational structure is in place defining areas of authority, responsibility, and lines of reporting. The structure is documented in current policies and organization charts that are available to all employees on the entity intranet. Reporting relationships and organization structures are reviewed annually by senior management as part of security organization planning and adjusted as needed based on changing entity commitments and requirements to ensure their continuing suitability, adequacy, and effectiveness.	Inspected policies and organization charts noting specification of authority, responsibility, and lines of reporting, as well as security management review and oversight.	No exceptions noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Inspected hiring policies and processes. Inspected a sample of roles identified in the organization chart and obtained job descriptions to determine whether the descriptions identified the responsibilities and authority for the selected roles.	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	Required skills, responsibilities, knowledge and experience levels are specified in position descriptions. Employee hiring procedures are in place that include verification that candidates possess the required skills, knowledge and experience to perform the duties defined in the job description. Employees are required to complete security awareness training when hired and on an annual basis thereafter. Management monitors training compliance.	Inspected hiring policies and processes. For a sample of employees, inspected personnel files to determine whether the candidate's skills, knowledge, and experience meet the requirements of the position, and whether these qualifications were verified and evaluated as part of the hiring or transfer process. Inspected the policy for annual security awareness training, recent training materials, and documentation of employee training.	No exceptions noted.
CC1.4	The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	The entity maintains a workforce code of conduct policy that delineates acceptable and unacceptable conduct, as well as a description of possible sanctions for violation of the policy. Personnel are required to read and accept the code of conduct and a statement of confidentiality and privacy practices upon their hire. Management monitors employees' compliance with the code of conduct through regular monitoring and review of employee information system activity. New personnel are offered employment subject to background checks.	Inspected workforce code of conduct policies and the code of conduct to determine whether it addresses acceptable and unacceptable conduct and possible sanctions. For a sample of new employees, inspected code of conduct acceptance documentation. Inspected records to determine whether a background check was performed. Inquired of management about the existence of any policy violations and sanctions implemented as a result of the violations.	**Exception noted:** One employee of 39 workforce candidates sampled did not complete the code of conduct acceptance documentation. **Nuance's Unaudited Response**: Nuance Healthcare agrees with the exception noted and has implemented process to address the issue.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC2.0	**Common Criteria Related to Communications**			
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	System documentation is available to authorized external and internal users that delineates the boundaries of the system and describes the purpose, design, and use of the system. Documentation is available as distributed documents or on the Internet for external users and on the intranet for internal users. Customers are provided with use and support guides that define roles and responsibilities, specify support points of contact, procedures, and processes for obtaining help, reporting issues, and tracking resolution of incidents.	Inspected documents and intranet/Internet descriptions of application systems to determine whether they provide adequate information on system design, purpose, and use; on customer responsibilities; and on customer support interfaces.	No exceptions noted.
CC2.2	The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	The entity security responsibilities are outlined in product descriptions, support guides, and administration guides. Detailed application information is available to entity staff on the intranet. Employees are required to complete security awareness training on an annual basis. Management monitors training compliance.	Inspected application descriptions, product support guides and application administration documents to confirm adequate descriptions of system capabilities and of entity staff responsibilities. Inspected the policies for annual security awareness training, recent training materials, and documentation of employee training. For a sample of employees, verified their attendance at annual training sessions.	No exceptions noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Internal operations staff, customer and end user security responsibilities are outlined in product descriptions, support guides, and administration guides. Detailed application information is available to staff on the entity intranet. Employees are required to complete security awareness training on an annual basis. Management monitors training compliance.	Inspected application descriptions, product support guides and application administration documents to confirm adequate descriptions of system capabilities and of operations staff and customer responsibilities. Verified employee security training.	No exceptions noted.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.	Employees are hired based on appropriate experience and knowledge as specified in formal job descriptions. Employees are required to complete security awareness training on an annual basis.	For a sample of employees hired or transferred to a new role during the period, obtained the file copy of their job description to determine whether the employees had appropriate background for their job responsibilities. Verified employee security training.	No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	The entity's security awareness program trains employees on how to identify and report possible security breaches. Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on customer support websites, in customer guides, and in system documentation. The incident management documents define the incident categorization, escalation, and resolution process.	Inspected customer support documents and websites to determine whether they provide sufficient information on reporting security issues. Inspected attendance sheets for the annual security training for employees and determined whether employees had signed the attendance sheet for the training session on those dates. Inspected the presentation material for relevant training sessions and determined whether the presentation material describes how to identify and report possible security breaches.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.	Proposed changes affecting internal staff and/or customers are communicated and confirmed with impacted parties through ongoing communication mechanisms. Changes that result from incidents are communicated to internal and external users through email as part of the implementation and closure process. Management must confirm understanding of changes by authorizing them. Some incidents cannot be resolved until they go through R&D of the product.	Inspected a sample of weekly changes and associated communications to determine whether all system changes were included and had been reviewed and signed off by the Change Advisory Board (CAB). Inspected incident documentation. Inspected Customer Support Center change-alert emails to customers to verify that notification had been provided of upcoming system changes and their impact on users, if any.	No exceptions noted.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
CC3.1	The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls), that could significantly affect the system of internal controls, and (5) reassess, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	The entity has defined risk management policies and processes implemented with the RSA Archer GRC (Governance, Risk, Compliance) Platform. The RSA Archer capability provides for: -Risk and threat assessments -Risk repository -Risk management processes -Issue management processes -Compliance audit/assessment findings list -Remediation plans -Repository and management of controls -Catalog of IT assets Vulnerability assessment and management is performed on an on-going basis.	Inspected the risk assessment policy and procedure definitions, documentation of the RSA Archer implementation and associated reports, and annual risk assessment documentation and reports to verify completeness of risk assessment, analysis, and mitigation. Examined a sample of vulnerability management reports and associated mitigations.	No exceptions noted.
CC3.2	The entity designs, develops, and implements and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	The entity has defined risk management policies and processes implemented with the RSA Archer GRC (Governance, Risk, Compliance) Platform. The RSA Archer capability provides for: -Risk and threat assessments -Risk repository -Risk management processes -Issue management processes -Compliance audit/assessment findings list -Remediation plans -Repository and management of controls -Catalog of IT assets	Inspected the risk assessment policy and procedure definitions and documentation of the RSA Archer implementation reports to verify definition and implementation of controls and processes for risk management and mitigation.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC4.0	**Common Criteria Related to Monitoring of Controls**			
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	External vulnerability assessments are performed on a monthly basis, and management initiates corrective actions for identified vulnerabilities. Monitoring software is used to identify and evaluate ongoing system performance, resource utilization, and unusual system activity or states. Alerts are sent to the Site Reliability Center for analysis and response. System/application logs are aggregated for analysis at the Security Operations Center. If appropriate, an incident and possibly a change management "ticket" record are created. Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inspected vulnerability assessments to determine whether they were performed on schedule. Inspected a sample of monitoring alerts sent to the Site Reliability Center (SRC) to verify active system monitoring. Inspected Sumo Logic logs and dashboard. Inspected a sample of identified corrective actions resulting from the vulnerability or monitoring processes to determine whether corrective actions were implemented.	No exceptions noted.
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Established entity standards exist for infrastructure and software hardening that include requirements for implementation of access control software. Logical access to entity systems and components is protected through the use of authentication services implemented with native operating system security, native application and resource security, and/or add-on security software. Administrative access to Active Directory, Linux/Unix, and the entity's servers, databases, storage, and network components is restricted to authorized employees. User activity is logged.	Inspected documentation of identification and authentication capabilities. Inspected server build specifications for completeness and conformity with security objectives. Inspected access control policies and processes. Inspected a sample of Active Directory, Linux/UNIX, and infrastructure component access control lists to determine whether access is restricted to appropriate employees based on their defined user role.	No exceptions noted.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	In order for the entity's employees to obtain system and component access, the employee's manager or supervisor must submit a request ticket which requires management review and approval. The request requires specification of the role and the required accesses. Unique user IDs are assigned to individual users. Access privileges may be assigned by role, by group, or in special cases individually. Access termination is triggered by an email from the human resources system to the HHIS Infrastructure Operations Team specifying employee termination. A request ticket is created to document and drive implementation of access termination. User status is audited quarterly. Customer users are defined and managed by customer administrators.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Inspected a sample of access request tickets to determine whether the request specified the individual, their role and required access and whether the access was approved by authorized staff. Examined a sample of access termination tickets. Examined application administration guides to verify client user administration capabilities.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Systems are configured to authenticate users with unique user accounts, passwords, certificates, or licenses and to enforce predefined user account and minimum password requirements as follows: • Passwords have a minimum of 8 characters, including 2 non-alphanumeric characters. • Passwords expire every 90 days for non-privileged accounts and 180 days for privileged accounts. • Log-on sessions terminate after 3 failed log-on attempts. • The last 10 passwords cannot be reused (5 passwords for privileged accounts). Account sharing is prohibited except for a minimized number of "root" like accesses, in which case mitigating controls are implemented when possible (for example, required use of "su" when accessing a UNIX root account). Customer users are required to have comparable unique identities, passwords, certificates, or licenses as determined by customer administrators.	Inspected password policies and their implementation via Active Directory and Linux/Unix based authentication services. Examined application administration guides to verify client user administration capabilities and capabilities to enforce password policy.	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	When possible, formal role-based access controls are created which limit access to system and infrastructure components. These are enforced by the access control system. When it is not possible, authorized user IDs must be members of an authorized access group, or be individually authorized. User access requests for a specific role are approved by the user manager and are submitted via a request ticket.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Reviewed a sample of access request tickets and the nature of the access that was established to confirm fulfillment of policy standards.	No exceptions noted.
CC5.5.1	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Physical access controls are in place to restrict access to and within data center facilities. A review of employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary.	Inspected policies, audit reports and other documentation of data center facilities to verify that physical access controls are in place that include the following: -Procedures have been established to restrict physical access to the data centers to authorized employees, vendors, contractors, and visitors. -Security verification and check-in are required for personnel requiring temporary access to the interior data center facility. -Physical access to the data center is reviewed quarterly and verified by the data center operations teams. -Physical access mechanisms (e.g. access card readers, biometric devices, man traps, portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. -The data center facilities are monitored 24/7 by security personnel.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	Criteria	Control Activity Specified by the Service Organization	Test Applied by Service Auditor	Results of Tests Performed
CC5.5.2		Employees and contractors are required to return their ID cards during exit interviews, and all ID badges are disabled prior to exit interviews. Therefore employees and contractors must be physically escorted from the entity's facilities at the completion of the exit interview. Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day. The sharing of access badges and tailgating are prohibited by policy.	Inspected a sample of exit interview records to verify that the badges of terminated employees or contractors have been returned and disabled.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	The entity uses firewalls to prevent unauthorized network access. Firewalls and other system mechanisms limit remote access and the types of activities and service requests that can be performed from external connections. External access is also restricted through the use of user authentication and message encryption systems such as VPN and SSL. Vulnerability scans are run monthly to detect and mitigate weaknesses.	Inspected network diagrams, system infrastructure descriptions, and data center audit reports to determine whether the system includes firewalls and other mechanisms to prevent unauthorized external access and to provide required encrypted customer access. For a sample of months, inspected the vulnerability assessment reports.	No exceptions noted.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes, and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and requirements as they relate to security, availability, and confidentiality.	VPN, SSL, and other encryption technologies are used for defined points of connectivity and to protect communications between a processing center and users connecting to a processing center from within or external to customer networks. The entity's customer web pages and services use HTTPS to encrypt communications over the Internet. By policy information system assets outside company facilities, including removable media containing EPHI and/or Personal Information, must be encrypted, physically secure when unattended and protected from environmental hazards. Backups are not written to removable media. Data retention and destruction policies and procedures are in place.	Inspected system infrastructure, network and product descriptions to verify use of encrypted communication paths. Inspected policies regarding copying of information to removable media. Inspected data retention and destruction policies and procedures.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	The ability to install software on systems is restricted to change implementation and system administration personnel acting with an approved change request. Antivirus software is installed on servers and signatures are kept current.	Inspected change management tickets to validate use of the change process to install code on production servers. Inspected a sample of server configuration reports to determine whether antivirus software was installed.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC6.0	**Common Criteria Related to System Operations**			
CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and new vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Vulnerability scans are executed and reviewed monthly. Logging and monitoring software is continuously active on infrastructure components tracking system performance, resource utilization, and unusual system activity and states. Monitoring software sends alerts to the Site Reliability Center. An incident may be opened in response to the alerts. Customer Support Center personnel receive customer telephone, email, or web messages, which may include notification of potential breaches and incidents. Customer Support Center staff follow defined protocols for recording, resolving, and escalating received reports.	Inspected the vulnerability management process. Inspected a sample of reports from the vulnerability scanning process. Inspected documentation of monitoring capabilities. Inspected a sample of alert notifications to the Site Reliability Center to determine whether monitoring software was operational.	No exceptions noted.
CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Customers and/or employees may identify issues to support staff who follow defined protocols for documenting, evaluating, and reporting incidents. Security related events are assigned to the security team for evaluation. When a critical incident is identified, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures and tracked through to resolution. Incidents that may affect security compliance / privacy are reported to the security compliance / privacy officials. The Corporate Privacy Officer and Vice President of Information Security are alerted of the incident and will participate as part of the Incident Management Team. Internal and external users are informed of incidents in a timely manner and advised of corrective measures to be taken on their part. Resolution of incidents is reviewed at incident management, operations, and security team meetings. Change management requests are opened for incident mitigations that require permanent fixes.	Inspected the incident management process. Inspected records of reported incidents. Inspected the instructions provided to staff and customers to determine whether they include protocols for communicating potential security breaches.	No exceptions noted.
CC7.0	**Common Criteria Related to Change Management**			
CC7.1	The entity's commitments and system requirements, as they related to security, availability, and confidentiality, are addressed during the system development lifecycle including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	As part of the change management process, change requests are evaluated to assess the impact of the change on security commitments and requirements.	Inspected the change management process. Inspected a sample of change requests to determine whether the changes were appropriately described, categorized, assessed, and approved by the security team prior to implementation.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Security Common Criteria				
CC#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	The entity maintains documented risk management, vulnerability/patch, and change management processes. During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. The vulnerability process drives near term changes. Plans and change requests are created based on the identified needs.	Inspected the security risk, vulnerability / patch, and change management processes to verify that there are documented policies and processes for addressing changing security requirements. Inspected the risk assessment and for a sample of months inspected the vulnerability reports, to determine whether issues were identified, evaluated, and mitigated, if appropriate.	No exceptions noted.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	For critical incidents, an analysis is performed and, based on the incident qualities, the critical incident management process may be invoked to resolve the identified issues. Other issues drive change through specific application/component channels. Based on analysis of the issue, change requests are prepared and implemented to address the root causes.	Inspected the analysis reports for critical incidents and the resulting change requests that were initiated to address deficiencies.	No exceptions noted.
CC7.4.1	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.	System change requests must be reviewed and approved by the owners of the software and the operational infrastructure, as represented on the Change Advisory Board (CAB), prior to work commencing on and then implementing the requested change. Changes are developed and tested in separate environments before implementation. All changes must include specification of acceptance criteria and back-out steps. Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented. Developers are not permitted to make changes independently in production environments.	Inspected the change management process to determine whether procedures are formally documented for authorization, approval, testing, and communication prior to implementation. Inspected a sample of change requests to determine whether the changes were authorized, approved, tested, and communicated prior to implementation, and that they specified acceptance criteria and back-out steps.	No exceptions noted.
CC7.4.2		The change process involves the following teams and their discrete responsibilities: • Change Advisory Board (CAB) - approval of change requests • Research & Development - application design and development • Professional Services - creation of initial customer configurations • Quality assurance and test teams - testing • HHIS teams - infrastructure and application deployment	Reviewed the change management process to verify clear definition of roles and responsibilities in the change process.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Additional Criteria for Availability				
A#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Processing capacity is monitored on an ongoing basis.	Inspected documentation of monitoring capabilities. Inspected a sample of monitoring reports showing Key Performance Indicators (KPI).	No exceptions noted.
A1.2		Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inspected data center configuration description and audit report. Inspected application configuration design documents.	No exceptions noted.
A1.3		Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by senior operations and development management. Change requests are initiated as needed based on approved forecasts.	Verified conduct of monthly performance / capacity review meetings and associated actions.	No exceptions noted.
A2.1	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Environmental controls have been implemented to protect systems inside the facility, including temperature and HVAC controls, fire detection and suppression systems, and power management systems. Established procedures are in place to provide continuity of telecommunications services.	Inspected data center audit report.	No exceptions noted.
A2.2		The data center facility is monitored 24/7 by security personnel.	Inspected data center audit report.	No exceptions noted.
A2.3		Data center management maintains managed equipment within the facility according to documented policy and maintenance procedures.	Inspected data center audit report.	No exceptions noted.
A2.4		Business continuity and disaster recovery plans have been established for data center managed components. The plans are tested on a regular basis and are updated annually. Application disaster recovery procedures have been established, are tested on a regular basis, and are updated as required.	Inspected disaster recovery plans. Inspected data center audit report. Inspected application backup and failover description. Inspected application failover test documentation.	No exceptions noted.
A2.5		The entity has contracted for two widely geographically separated facilities which host two active-active instances of the application providing for rapid failover with minimal data loss.	Inspected data center audit report. Inspected application backup and failover description. Inspected application failover test documentation.	No exceptions noted.
A2.6		Critical data is replicated multiple times at both data centers and is also geo-replicated to the alternate site. Less critical data is replicated multiple times within each data center. Transaction log backups are saved every few minutes with a full backup taken nightly.	Inspected application backup and failover description.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Additional Criteria for Availability				
A#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
A3.2		Test results are reviewed and the contingency plan is adjusted.	Inspected application backup and failover description. Inspected application failover test documentation.	No exceptions noted.
Additional Criteria for Confidentiality				
C#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Production and non-production design, development, and test environments have the same controls for protection of confidential information.	Inspected infrastructure descriptions. Inspected application architecture and functional descriptions, application support, and administration processes to confirm adequate protection mechanisms and procedures.	No exceptions noted.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Application, data management, network and operating system security restrict the ability to access, modify, and delete data to authorized and authenticated applications and users. Creation and modification of access control rules is managed through the access provisioning and termination processes.	Inspected infrastructure descriptions. Inspected application architecture and functional descriptions, application support, and administration processes to confirm adequate protection mechanisms and procedures.	No exceptions noted.
C1.3.1	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with the entity's confidentiality commitments and system requirements.	Application and system security restrict access and output to approved and authenticated users and devices.	Inspected system infrastructure, network, and application descriptions, and support procedures to verify use of authentication mechanisms and encrypted communication paths.	No exceptions noted.
C1.3.2		Transmission of digital output beyond the boundary of the system occurs through the use of authorized software supporting approved encryption algorithms.	Inspected policies and procedures regarding transmission of information and copying of information to removable media.	No exceptions noted.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services comprise part of the system and have access to confidential information.	Formal information protection agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity.	Inspected policies regarding confidentiality. Inspected vendor agreements regarding confidentiality.	**Exception noted**: One agreement of three agreements selected for testing was not located. **Nuance's Unaudited Response:** Nuance healthcare agrees with the exception noted and has implemented process to address the issue.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and other third parties whose products and services are part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.	Related third party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated.	Inspected data center SOC2 reports to verify data center security measures.	No exceptions noted.
C1.6.1	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	The chief information security officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to employees, users, related parties, and vendors.	Inspected policies and materials regarding confidentiality, required employee acknowledgment of confidentiality of protected information, and inclusion of confidentiality in required security training.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

Additional Criteria for Confidentiality				
C#	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by Service Auditor**	**Results of Tests Performed**
C1.6.2		Related party and vendor agreements are modified to reflect changes in confidentiality practices and commitments.	Inspected security policy change process.	No exceptions noted.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Inspected application architecture and functional descriptions, application support, and administration processes to confirm adequate protection mechanisms and procedures.	No exceptions noted.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	Reviewed data destruction policy and procedures. Inspected documents identifying confidential information being destroyed according to policy.	No exceptions noted.