US Signal Company, LLC

System and Organization Controls (SOC) 2 Type 2

Report on US Signal Company, LLC's Description of Its Network and Data Center Services System and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality and the Applicable Administrative, Physical, and Technical Safeguards as Set Forth in the HIPAA Security Rule

Throughout the Period
July 1, 2022 to June 30, 2023

Contents

I. Independent Service Auditor's Report on a SOC 2 Examination 3

II. Assertion of US Signal Company, LLC Management 8

III. US Signal Company, LLC's Description of Its Network and Data Center Services System 11

IV. Trust Services Criteria, Applicable Requirements of the HIPAA Security Rule, Related Controls, Tests of Controls, and Results of Tests 28

I. Independent Service Auditor's Report on a SOC 2 Examination

Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 South Hanley Road
Suite 800
St. Louis, MO 63105

Independent Service Auditor's Report on a SOC 2 Examination

To the Management of
US Signal Company, LLC
Grand Rapids, Michigan

Scope

We have examined US Signal Company, LLC's (US Signal or service organization) accompanying description of its network and data center services system (the system) titled *US Signal Company, LLC's Description of Its Network and Data Center Services System* throughout the period July 1, 2022 to June 30, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that US Signal's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. We have also examined the suitability of the design and operating effectiveness of controls to meet the applicable administrative, physical, and technical safeguards as set forth in the Health Insurance Portability and Accountability Act (HIPAA), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (applicable requirements of the HIPAA security rule) throughout the period July 1, 2022 to June 30, 2023. Our examination does not provide a legal determination on US Signal's compliance with laws and regulations related to the applicable requirements of the HIPAA security rule throughout the period July 1, 2022 to June 30, 2023.

US Signal uses several Point of Presence facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at US Signal, to achieve US Signal's service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule. The description presents US Signal's controls, the applicable trust services criteria, the applicable requirements of the HIPAA security rule, and the types of complementary subservice organization controls assumed in the design of US Signal's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

US Signal is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that US Signal's service commitments and system requirements were achieved. US Signal has provided the accompanying assertion, titled *Assertion of US Signal Company, LLC Management* (assertion), about the description and the suitability of the design and operating effectiveness of

controls stated therein. US Signal is also 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; selecting the applicable trust services criteria and the applicable requirements of the HIPAA security rule and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects:

a. The description presents US Signal's network and data center services system that was designed and implemented throughout the period July 1, 2022 to June 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that US Signal's service commitments and system requirements would be achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of US Signal's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that US Signal's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule if complementary subservice organization controls assumed in the design of US Signal's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of US Signal, user entities of US Signal's system during some or all of the period July 1, 2022 to June 30, 2023, business partners of US Signal subject to risks arising from interactions with the system, practitioners providing services to such user

entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria and the applicable requirements of the HIPAA security rule.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, 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.

BDO USA, P.C.

September 21, 2023

II. Assertion of US Signal Company, LLC Management

Assertion of US Signal Company, LLC Management

We have prepared the accompanying description of US Signal Company, LLC's (US Signal or service organization) network and data center services system (the system) titled *US Signal Company, LLC's Description of Its Network and Data Center Services System* throughout the period July 1, 2022 to June 30, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with US Signal's system, particularly information about system controls that US Signal has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria* and the applicable administrative, physical, and technical safeguards as set forth in the Health Insurance Portability and Accountability Act (HIPAA), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (applicable requirements of the HIPAA security rule).

US Signal uses several Point of Presence facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at US Signal, to achieve US Signal's service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule. The description presents US Signal's controls, the applicable trust services criteria and the applicable requirements of the HIPAA security rule, and the types of complementary subservice organization controls assumed in the design of US Signal's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. The description presents US Signal's network and data center services system that was designed and implemented throughout the period July 1, 2022 to June 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that US Signal's service commitments and system requirements would be achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of US Signal's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that US Signal's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule if complementary subservice organization controls assumed in the design of US Signal's controls operated effectively throughout that period.

US Signal Company, LLC

September 21, 2023

III. US Signal Company, LLC's Description of Its Network and Data Center Services System

US Signal Company, LLC's Description of Its Network and Data Center Services System

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of US Signal Company, LLC's (US Signal, service organization, or Company) network and data center services system (the system) and the controls in place to provide reasonable assurance that US Signal's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria* and the applicable administrative, physical, and technical safeguards as set forth in the Health Insurance Portability and Accountability Act (HIPAA), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (applicable requirements of the HIPAA security rule), throughout the period July 1, 2022 to June 30, 2023 (the period), which may be relevant to the users of the system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by US Signal.

The following requirements of the HIPAA Security Rule been deemed not applicable for US Signal's environment:

Applicable Requirement of the HIPAA Security Rule	Reason for Not Being Applicable
164.308(a)(4)(ii)(A) Isolating Clearinghouse	US Signal does not perform clearinghouse activities.
164.314(a)(1) Business Associate Contracts or Other Arrangements	US Signal does not allow business associates to interact with personal health information (PHI) in the US Signal environment.
164.314(a)(2)(i) Business Associate Contracts	
164.314(a)(2)(ii) Other Arrangements	
164.314(b)(1) Requirements for Group Health Plans	US Signal does not serve as a health plan sponsor.
164.314(b)(2) (i) Implementation Specification	
164.314(b)(2) (ii) Implementation Specification	
164.314(b)(2) (iii) Implementation Specification	
164.314(b)(2) (iv) Implementation Specification	

In addition to US Signal's headquarters in Grand Rapids, Michigan, the system's scope includes the following US Signal data center facilities:

Michigan	Indiana	Illinois	Wisconsin
Detroit Metro	Indianapolis	Oak Brook	Madison
Grand Rapids East	South Bend		
Grand Rapids South			
Southfield			

US Signal uses several Point of Presence (POP) facility landlords, subservice organizations, to provide secure facilities for connectivity points. The description only includes the controls of US Signal and does not disclose the actual controls at the subservice organizations.

On February 14, 2023, US Signal was acquired by Igneo Infrastructure Partners. US Signal remains an independent entity and is responsible for the services to its clients as well as the controls related to the network and data center services system as it pertains to the scope of this report. Controls performed by Igneo Infrastructure Partners are not included in the scope of this report.

Company Background

US Signal is a digital infrastructure company offering network connectivity, cloud hosting, colocation, data protection, security, and disaster recovery solutions, all powered by its wholly owned and operated robust fiber network. US Signal also helps customers optimize their information technology (IT) resources through managed and professional services.

Services Provided

The Company's product and service offerings include cloud hosting, colocation, data protection, security, and disaster recovery solutions in addition to its network services.

Principal Service Commitments and System Requirements

US Signal's principal service commitments and system requirements are documented and communicated to customers within master service agreements (MSAs). Additionally, US Signal has formalized service level agreements (SLAs) by service offering that are documented and made available to customers on the US Signal website.

Service commitments and system requirements vary based on the services being provided; however, common commitments and system requirements in place include the following:

- Data centers will be equipped with HVAC equipment.
- Data centers will contain clean-agent fire suppression systems.
- US Signal will maintain its software and hardware.
- US Signal will comply with its data security policies and procedures and applicable privacy laws.
- US Signal will maintain 100% resource pool, flexible resource pool, cloud load balancer, and file storage availability.
- US Signal will maintain 99.99% object storage availability.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in US Signal's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In determining whether a system incident occurred resulting in US Signal's failure to achieve one or more of its service

commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to US Signal's service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a system incident has occurred; however, incidents and events relevant to US Signal's service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to US Signal's service commitments and system requirements based on the applicable trust services criteria will make that determination.

US Signal did not identify any system incidents that occurred during the period July 1, 2022 to June 30, 2023 resulting in US Signal's failure to achieve one or more of its service commitments or system requirements based on these considerations.

Components of the System Used to Provide the Services

Infrastructure

US Signal uses multiple methods to keep management and customer traffic separate and provide a secure and redundant network architecture. These methods include virtual routing and forwarding (VRFs) and virtual local area networks (VLANs) or even separate physical networks where appropriate. Network engineers monitor network components for security, capacity, and performance issues. Additional control procedures include:

- Full infrastructure redundancy for routers, switches, firewalls, and other network components.
- Secure, hardened operating systems.
- Real-time monitoring and reporting tools.
- Capacity planning and utilization monitoring.

Software

US Signal uses Active Directory to control network access and access to internal systems. Desktop systems utilize SentinelOne and CrowdStrike to protect against viruses. US Signal encrypts the drive of employee laptops with BitLocker.

OMNI is an order management tool used by US Signal employees to manage customer requests, including new orders or changes to existing products. The OMNI application also has built-in ticketing functionality for supporting customer systems and customer impacting change management. The ticketing functionality was migrated to Salesforce Service Cloud in September 2022.

US Signal uses a helpdesk ticketing system for new user access requests, termination access removal tracking, and internal system change management tasks. The Fresh Service ticketing application was used for this; however ticketing was migrated to the Salesforce Service Cloud ticketing application beginning in May 2022 and completed in October 2022.

The Customer Portal is a web-based portal that allows customers to login and submit requests and/or tickets directly to US Signal. The portal is integrated with the OMNI application.

US Signal uses the Git source-code repository application to manage the application code to the customer portal.

People

US Signal is committed to equal opportunity employment and employment decisions based on merit, qualifications, and abilities. US Signal endorses a work environment free from discrimination and harassment. Company policy prohibits unlawful discrimination based on race, color, creed, gender, marital status, age, national origin or ancestry, physical or mental disability, medical condition, veteran status, or any other consideration made unlawful by federal, state, or local laws.

US Signal is committed to complying with all applicable laws providing equal employment opportunities. This commitment applies to all persons involved in the operations of US Signal and prohibits unlawful discrimination by any employee of US Signal, including management and co-workers.

US Signal has a staff of approximately 190 employees to deliver the network and data center services system.

US Signal has formal hiring practices designed to ensure that new employees are qualified to carry out their job responsibilities. New-position hiring is jointly coordinated by the Human Resources (HR) Department and the respective Department Manager. Hiring policies require candidates to have an education and experience level appropriate to their job function.

From July 1, 2022 through February 13, 2023, the Executive Security Team provided leadership in the protection of US Signal and customer information assets and technology. The Executive Security Team members advised on and helped prioritize the development of information security policies, initiatives, and projects utilizing a risk-based approach. The Executive Security Team also provided guidance and leadership to maintain and improve the security and availability of data created or housed by US Signal. As of February 14, 2023, the Executive Leadership and US Signal Board of Directors assumes the ongoing responsibility for the US Signal Information Security program.

Processes and Procedures

Policies and procedures at US Signal are maintained by management and are reviewed and updated as necessary or on an annual basis. The policies are approved by the Chief Information Security Officer or Department Manager. The policies and procedures provide guidance to employees and serve as a foundation for detailed divisional and departmental policies and procedures. The

automated and manual procedures involved in the operation of the system, including how services are initiated, authorized, performed, and delivered in a secure manner, are included in the system description, including the following policy and procedure documents:

- Information Security Policy
- Corporate Acceptable Use Policy
- Incident Response Policy
- Data Protection Policy
- Data Sanitization Policy
- Vendor Management Policy
- Business Continuity and Disaster Recovery Manual
- Employee Handbook

Data

Customer data is managed and stored in accordance with applicable data protection and privacy regulations, with specific requirements formally established in customer contracts. Customer data is logically isolated, monitored, and security-hardened. Data encryption is performed on sensitive customer data at rest. US Signal offers services capable of encryption for data in transit.

Description of the Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories and the Applicable Requirements of the HIPAA Security Rule

Numerical cross-references are used to reference controls in the following portion of Section III to the related control and testing in Section IV.

Control Environment

Commitment to Integrity and Ethical Values

US Signal has a documented Business Conduct Policy within the Employee Handbook that defines employee conduct standards. The Employee Handbook is posted on the intranet and made available for employees to view (CC1.1.1). Employees are required to sign an acknowledgement stating they have read, understand, and agree to comply with the responsibilities and requirements outlined within the Employee Handbook and US Signal policies upon hire and annually thereafter (CC1.1.2).

Individuals offered positions at US Signal are subject to background checks as part of the employee screening process (CC1.1.3).

US Signal has an anonymous policy-violation complaint form available to internal users on the intranet. Compliance Management is automatically notified and monitors workforce member complaints reported via the form (CC1.1.4).

Independent Oversight

From July 1, 2022 through February 13, 2023, the Chairman, Chief Executive Officer (CEO), and Managing Member of US Signal was independent of the day-to-day operations of control owners and served in an oversight capacity of the line management overseeing those control owners (CC1.2.1). The Chief Information Security Officer provided oversight of the development and performance of internal control during that time through oversight of the Internal Audit Program and the Information Security Program, which drove the execution of US Signal's Governance, Risk, Compliance, and Security Program. The Chief Information Security Officer reported results directly to the Chairman, CEO, and Managing Member of US Signal during this time (CC1.2.3).

Once US Signal was acquired by Igneo Infrastructure Partners on February 14, 2023, a formal Board of Directors was put in place. The roles and responsibilities of the US Signal Board of Directors are segregated from the roles and responsibilities of management. The Board is independent of the day-to-day operations of control owners and serves in an oversight capacity of the line management overseeing those control owners (CC1.2.2). In addition, the US Signal Board of Directors has established an audit subcommittee, which is responsible for oversight of the Internal Audit and Information Security Programs at US Signal (CC1.2.5). The Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis (CC1.2.6). During these meetings the Chief Information Security Officer provides oversight of the development and performance of internal control through oversight of the Internal Audit Program and the Information Security Program, which drives the execution of US Signal's Governance, Risk, Compliance, and Security Program. The Chief Information Security Officer reports results directly to the Board of Directors of US Signal (CC1.2.4).

Organizational Structure

US Signal maintains an up-to-date organizational chart that outlines reporting lines and levels of authorities within the organization. The organizational chart is posted within the HR information system and made available for employees to view (CC1.3.1). The roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description (CC1.3.2). The responsibility and accountability for updating and maintaining US Signal information security policies are assigned to the Chief Information Security Officer and executive leadership. US Signal policies are reviewed annually and updated as necessary (CC1.3.3).

Resource Planning

On an at least annual basis, management performs people and resource planning to ensure appropriate staff and resources are available to meet the Company's objectives and presents to the Board of Directors for approval (CC1.4.1). If it is determined that additional resources are needed, the new hire and/or asset acquisition processes are initiated.

Employee Performance and Training

Employee performance is evaluated on an annual basis to determine that employees are qualified to fulfill their job responsibilities (CC1.4.2). Employees are also required to complete security awareness training when hired and on an annual basis thereafter (CC1.4.3). If an individual is deemed to not be meeting the qualifications of the job position, including not completing necessary

trainings, US Signal has a documented Progressive Discipline Policy within the Employee Handbook, which is used to outline procedures around how they address conduct issues. When conduct issues occur, a discipline form is completed to document the issue and is signed by the employee, their supervisor, and HR (CC1.5.1).

Communication and Information

US Signal has implemented policies and procedures relevant to information security, and based on those policies and procedures, performs logical and physical security, change management, incident monitoring, and retention control activities, to ensure that the systems supporting the functioning of internal control are producing relevant, quality information (CC2.1.1).

Internal Communication

US Signal uses various methods of communication within the Company to ensure that employees understand their individual roles and responsibilities as they relate to the network and data center services. These methods include orientation and training, the use of electronic mail messages to communicate time-sensitive information, systems of record, and the use of diagnostic applications to monitor services and automatically alert staff when issues arise.

Descriptions of US Signal's systems are posted on the Company's intranet and are available to internal users to view. The descriptions delineate the boundaries of the systems and key aspects of processing (CC2.1.2).

To communicate the incident response procedures to internal users, US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view (CC2.2.1). US Signal has also implemented formal customer support and incident management policies and procedures that document how customer service issues are handled. The policy is posted in the US Signal file directory and available for internal users to view (CC2.2.2).

In order to ensure that internal users are aware of changes that are being made within the environment, US Signal maintains a system-change calendar that identifies and communicates planned changes throughout the year. It is posted and available for internal users to view through a shared Microsoft (MS) Outlook calendar (CC2.2.3). System changes that affect US Signal services are communicated to applicable internal and external users as part of the implementation process (CC2.2.4).

External Communication

System descriptions are available to external users through the customer portal that delineate the boundaries of the system and describe relevant components, as well as its purpose and design (CC2.3.1). Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners (CC2.3.2). In addition, products and services offered by US Signal have documented SLAs that are made available to customers on the US Signal website (CC2.3.3).

US Signal's security, availability, and confidentiality responsibilities and commitments are communicated to external users within master agreements (CC2.3.4).

Customers are provided information on how to report security events and service-related issues via phone, email, or through creating a trouble ticket through the customer portal to the Technical Operations Center (TOC) on the US Signal website (CC2.3.5).

Risk Assessment

US Signal recognizes the importance of risk management in properly managing corporate and customer assets and providing high-quality, cost-effective services to its customers. To assist with this, management maintains a list of objectives and contractual commitments that is reviewed and updated on at least an annual basis to ensure that they are documented with sufficient clarity (CC3.1.1). US Signal monitors service-level statistics on a quarterly basis to ensure that they are meeting company objectives. Results of the monitoring are communicated to management for review (CC3.1.2).

Management subscribes to external reporting services that identify changes to technology or regulations relating to services provided by US Signal (CC3.1.3). Additionally, the Information Security Team maintains an Information Security and Compliance road map that outlines the IT strategic objectives and projects. The road map is reviewed and updated by management on an at least annual basis (CC3.1.4).

US Signal performs a risk assessment over their environment on an annual basis to identify potential threats that would impair system security and availability and analyze the risk associated with the identified threats and determine mitigation strategies for those risks (CC3.2.1). From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks (CC3.2.2). In addition to the overall risk assessment, US Signal has documented risks for each line of business to identify potential vulnerabilities and threats specific to each service they provide. The product-specific risk assessments are updated on an as-needed basis (CC3.2.3).

As part of the annual risk assessment, management assesses fraud risk to identify the various ways that fraud and misconduct can occur within their environment, including how management might engage in inappropriate actions, and maintains documentation of this assessment (CC3.3.1).

Through its ongoing and annual risk-assessment process, US Signal evaluates changes in the regulatory and physical environment in which US Signal operates, as well as vendor and business-partner relationships (CC3.4.1).

Monitoring Activities

Management performs ongoing evaluations on a day-to-day basis to monitor the effectiveness of controls and functions of the organization. From these evaluations, US Signal develops an audit schedule annually to assist with identifying and monitoring the various levels of risk within the organization (CC4.1.1). Based on the audit schedule, US Signal performs various self-certification audits annually to test the design and operating effectiveness of controls within the environment. Audit reports are generated to document their procedures and results of the self-certification audits (CC4.1.2). US Signal performs an internal assessment of their controls against the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) on at least an annual basis. Results of the assessment are reviewed by management to ensure that components of internal controls are present and functioning (CC4.1.3).

In addition to the audits above, US Signal audits their data center facilities on an annual basis to ensure that the appropriate controls are in place and operating effectively at the facilities (CC4.1.4).

The results of internal assessments are communicated to the CEO or executive leadership at least annually (CC4.2.1).

Control Activities

As part of its annual risk assessment, management links identified risks to controls that have been designed and implemented to address them (CC5.1.1).

When US Signal identifies the need for new controls, management considers a mix of control activities, including both manual and automated controls and preventive and detective controls. US Signal uses NIST as a framework to select and develop general control activities in the areas of security administration, application change control, systems development life cycle, and computer operations (CC5.2.1). Based on this framework, US Signal selects logical and physical security, change management, and incident monitoring control activities to manage technology infrastructure and security access risks identified during the annual risk assessment process (CC5.2.2).

Additionally, from July 1, 2022 through February 13, 2023, US Signal monitors their asset inventory via their Information Security and Compliance scorecard. The scorecard is updated and reviewed as part of the monthly Executive Security Team meetings (CC5.2.3). Beginning February 14, 2023, on a quarterly basis, US Signal monitors their asset inventory and results are reported to management for review (CC5.2.4).

Logical and Physical Access

Logical Security Software, Infrastructure, and Architecture

Customer data storage is segregated into individual virtual storage repositories so that customers do not have access to other customers' data (CC6.1.1).

US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization (CC6.1.2). The firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the intrusion detection system/intrusion prevention system (IDS/IPS) tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats (CC6.1.3).

Access to the individual production network elements and managed Customer Premise Equipment (CPE) is authenticated through a centralized RADIUS server (CC6.1.4). Access to production network elements is configured to be restricted to specific protocols, ports, and IP addresses (CC6.1.5). Access to the RADIUS server, which restricts access to the production network elements, is configured to authenticate via Active Directory (CC6.1.6). In accordance with the US Signal Information Security Policy, users with access to US Signal systems require a uniquely assigned identifiable user ID (CC6.1.7).

Network password restrictions are enabled for password length, strength, duration, history, and lockout settings (CC6.1.8). Additionally, OMNI password parameters are in place and are set to require minimum length, complexity, expiration, history, and lockout settings (CC6.1.9).

Access Provisioning and Deprovisioning

When a new user needs access to the production network or managed data center elements, HR personnel or Department Managers submit requests for access to the production network elements to the IT Helpdesk who validate the request was properly authorized and configure access in the production (RADIUS) server (CC6.2.1). Access to the production network elements is limited to the roles and positions that have been identified as requiring it.

When a user needs access to the network, HR personnel or Department Managers submit requests for new-user access to the domain to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates the new user's accounts with the appropriate access based on the user's role and access requested (CC6.2.2). Additionally, when a user needs access to internal systems, HR personnel or Department Managers submit requests for new user access to the OMNI application to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates or modifies the user's account with the appropriate access based on the user's role and access requested (CC6.2.3). Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel (CC6.2.4).

Privileged Access — Managed Data Center

Users with the ability to access the vSphere are limited to authorized and appropriate IT personnel based on job responsibilities (CC6.3.1).

Privileged Access and Access Review — Corporate Network and Internal Systems

The ability to create or modify users and user access privileges is limited to authorized and appropriate IT personnel based on job responsibilities (CC6.3.2).

Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management (CC6.3.3).

Additionally, user access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management (CC6.3.4).

Physical Access

Access to the corporate headquarters and data center facilities containing production servers and telecommunication equipment is controlled and restricted by an electronic proximity card or biometric access system (CC6.4.1). In addition to the electronic proximity card or biometric access system, the data center facilities' camera and alarm systems are monitored on an ongoing basis by the TOC. Camera and alarm systems are in place at each data center facility to ensure each location is secured and monitored (CC6.4.2).

Granting access to the data center facilities follows two processes, depending on who is requesting the access. For employees, requests for new access or changes to existing access are submitted to the Facilities Department from HR personnel. For customers and vendors, requests for new access or changes to existing access are submitted to the Facilities Department from the customer's or vendor's designated point of contact. The Facilities Manager validates the request and creates the new user's access based on the request (CC6.4.3). When employees leave the organization, HR personnel reclaim the terminated employee's access card and notify the Facilities Manager via email or ticket so that physical access privileges, such as biometrics or proximity card, will be revoked (CC6.4.4). Customers are responsible for notifying US Signal when physical access should be terminated for their employees. When US Signal receives a request for removal of customer access to the data center, a ticket is created to track the removal of physical access (CC6.4.5).

Physical access to the corporate headquarters and data center facilities is reviewed on a quarterly basis by management. Any access modifications needed as a result of the review are made by management (CC6.4.6).

Asset Disposal

US Signal has formal data retention and disposal procedures are in place to guide the secure disposal of the Company's and customers' data (CC6.5.1). Equipment potentially storing digital media is degaussed, sanitized, and/or securely destroyed prior to the equipment being removed from the US Signal facility or data centers (CC6.5.2).

Network Segmentation and VPN

The US Signal production network elements are managed via an out-of-band network that is segregated from the carrier transport network to ensure separation of the management and production network (CC6.6.1).

Remote access to the US Signal internal network is permitted for Active Directory users via virtual private network (VPN) connectivity with Duo security two-factor authentication connectivity (CC6.6.2).

Encryption and Data Loss Prevention

US Signal uses Wi-Fi Protected Access 2 (WPA2) encryption on wireless network connections, and access is limited to Active Directory users (CC6.7.1). US Signal's Information Security Policy prohibits the transmission of sensitive information over the internet or other public communications paths (for example, email), unless it is encrypted (CC6.7.2). Data Loss Prevention (DLP) software scans for sensitive information in outgoing transmissions over public communication paths. Information that is restricted is blocked from outgoing transmissions (CC6.7.3). Additionally, the storage for workstations and laptops is encrypted at rest via BitLocker (CC6.7.4). Removable media for workstations and laptops are also encrypted automatically by the software (CC6.7.5).

Antivirus

Antivirus software protects production and email servers, workstations, and network-connected laptops against viruses and other malicious code (CC6.8.1). The antivirus software is configured to monitor data and traffic on production and email servers, workstations, and network-connected laptops with virus signature definitions that are automatically updated from the vendor (CC6.8.2). US Signal has a predefined listing of software that is prohibited from being installed on company

laptops and workstations. Software on the predefined listing is automatically uninstalled, and IT is alerted (CC6.8.3).

System Operations

The Information Technology Department leverages nationally recognized IT and security frameworks, such as NIST, and utilizes various solutions to evaluate the design and operating effectiveness of its controls on a periodic basis. Internal and external vulnerability scans are performed on at least a quarterly basis, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements. Vulnerabilities identified from the scans are reviewed by management to ensure that they are being tracked and resolved in a timely manner (CC7.1.1). Additionally, a network segmentation test is performed on an annual basis and identified failures from the test will result in a finding within the report. If failures are identified from the test, the Information Security Team will further investigate and resolve the issue (CC7.1.2). Penetration testing is also performed on an annual basis. Critical and high-risk findings identified from the tests are tracked and resolved (CC7.1.3). System firewall audits are conducted on at least a biannual basis to validate firewall configurations are appropriate (CC7.1.7).

Logging and monitoring of security events are enabled on network elements and are configured to log activity to an internal security information and event management (SIEM) and the Company's Network Management System (NMS) (CC7.1.4). In addition to the logging and monitoring of security events on network elements, potential Active Directory security violations, including users gaining administrative access to the system, are logged within the SIEM (CC7.1.5).

Security events from the NMS are monitored in real time by the TOC (CC7.1.6). TOC personnel document service issues that have been identified and reported to them through the NMS or by internal and external users within a ticketing system. TOC personnel review the issue and close a ticket once the item has been addressed (CC7.3.1). Security events are documented within Service Cloud tickets. Security Operations Center personnel review Service Cloud tickets to determine if the events have been resolved, or if they need to be investigated further as an incident (CC7.3.2).

If a security event is believed to be a potential security, availability, or confidentiality incident (incident), management is notified to investigate it. If it is deemed that an incident has occurred, the Incident Response Policy is initiated. Identified security, availability, or confidentiality incidents are documented and tracked within incident response reports. US Signal researches the potential impact of the identified incident and documents how it was resolved within the report (CC7.4.1).

After an incident has been mitigated or resolved, a root-cause analysis of the incident is performed to ensure that the appropriate activities are implemented to recover from the incident (CC7.5.1).

Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure that the incident response procedures are up to date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents (CC7.5.2).

Change Management

US Signal has a formalized Data Protection Policy posted on their intranet to guide personnel in the design, testing, and implementation of systems (CC8.1.1). Development/staging environments are separated from production environments (CC8.1.2).

Management meets on a weekly basis to review and discuss past, in-progress, and upcoming changes, as well as current project status and development statistics (CC8.1.3).

Infrastructure

Requests to implement new or change existing customer equipment are documented within project checklists, where a project manager verifies the appropriate steps are completed based on the type of request, including testing and authorization by the customer (CC8.1.4). Changes to US Signal's internal infrastructure are documented within tickets and approved prior to the change being made (CC8.1.5).

Application and Database Development

Project changes are requested by the business via email or a ticket. Once requested and approved, the project is documented and logged into the backlog to begin development (CC8.1.6). Once development has been completed, project code changes are reviewed by a peer programmer who was not responsible for the change prior to the change being deployed to production (CC8.1.7). If the peer code review is passed, the project changes are tested by the business prior to the change being implemented into production (CC8.1.8). Testing results are communicated back to the development team via email. If any additional changes are needed based on results of the tested changes, they are communicated and tested again prior to going into production.

Minor/emergency code changes are documented within tickets and reviewed by a peer programmer who was not responsible for the change prior to the change being placed into production (CC8.1.9).

Access to deploy changes to production is limited to appropriate users and segregated from access to development, except for two select users who require access to both environments in order to support customer requests. Where access is required to both environments, changes to source code made by those users require a secondary review and approval prior to the code being deployed (CC8.1.10). Notifications are also configured within GitHub to alert the US Signal software development team of and changes that are made (CC8.1.11). In addition, beginning January 9, 2023, logging and monitoring of GitHub are configured to log activity to an internal SIEM. Any GitHub changes that require investigation are documented within event tickets. Security Operations Center personnel review tickets to determine if the events have been resolved, or if they need to be investigated further as an incident (CC8.1.12).

Risk Mitigation

US Signal has developed a risk-management program. The risk-management program includes the use of insurance to minimize the financial impact of any loss events (CC9.1.1).

Additionally, US Signal has a documented Vendor Management Policy that outlines their vendor due-diligence procedures. Based on the policy, US Signal performs annual due diligence on high-risk vendors to ensure that the risk associated with vendors is managed (CC9.2.1).

Description of the Additional Controls Relevant to the Availability Trust Services Category

Monitoring

US Signal's equipment that monitors managed CPE is configured to log and trap link status to the NMS. If a managed CPE does not communicate to the monitoring equipment, the link status of the CPE is logged in the NMS, and the TOC receives the underlying Managed Service Alarm(s) and responds in accordance with established policies and procedures to ensure that the stated SLA for the service is provided (A1.1.1). Additionally, managed data center physical hardware, software, and network elements are configured to be monitored for availability using the NMS. The NMS has been configured to alert TOC staff in the event that a piece of physical hardware, software, or element becomes unavailable (A1.1.2). US Signal monitors capacity within the environment on a monthly basis. Monitoring performed includes, but is not limited to, power usage, floor and cabinet space, storage capacity, and bandwidth metrics (A1.1.3).

Backups

US Signal has numerous backup configurations set up based on the type of data being captured. Backups of the OMNI application databases are performed utilizing replication utilities. Backups are automatically monitored for errors and, if any, an alert is sent (A1.2.1). Active Directory domain data is electronically replicated on a real-time basis from the servers in Grand Rapids, Michigan to another US Signal facility (A1.2.2). Additionally, an incremental backup of production network router configurations is performed on a daily basis (A1.2.3). The backup system sends a Daily Node Backup report to the Transport Engineering email distribution group indicating the number of node backups attempted and any failures that occurred (A1.2.4).

Environmental Protections

Fire and smoke detectors, automated clean-agent or pre-action wet fire suppression systems, and hand-held fire extinguishers are in place to protect US Signal data center facilities from fire-related hazards (A1.2.5). The data center facilities feature dedicated climate control systems to control the temperature and humidity within the facilities (A1.2.6). Additionally, uninterruptible power supply (UPS) units and power generation equipment protect the server and telecommunication equipment from power surges and sudden power outages (A1.2.7).

Disaster Recovery and Business Continuity

A Business Continuity and Disaster Recovery Manual has been established, and the manual is reviewed and tested at least annually (A1.2.8). Outside of the disaster recovery test process, a restore test on backups is performed on at least an annual basis to test the recoverability of backups (A1.3.1).

Description of the Additional Controls Relevant to the Confidentiality Trust Services Category

US Signal has a Client Data Retention Requirements Policy that documents the requirements for retaining confidential information. US Signal performs a quarterly data retention and destruction audit to ensure data retention and destruction procedures are being followed (C1.1.1).

US Signal's office location is equipped with locked shredding containers to allow for employees to properly dispose of confidential information (C1.1.2). Additionally, upon customer request or the termination of a customer contract, US Signal will destroy the customer data in accordance with the Data Protection Policy (C1.2.1).

Description of the Additional Controls Relevant to the Applicable Requirements of the HIPAA Security Rule That Do Not Overlap with SOC 2 Criteria

US Signal maintains a log of repairs and modifications to the physical components of the facilities related to security (H1.1). Employees are instructed as to the proper use of workstations, hardware, and electronic media via the Corporate Acceptable Use Policy (H2.1).

A Business Impact Analysis (BIA) is performed on an annual basis to document the potential effects of an interruption to critical business operations (H3.1).

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that US Signal's management assumed, in the design of the system, would be implemented by a subservice organization and are necessary, in combination with controls at US Signal, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Criteria
Point of Presence Facility Landlords		
1.	Physical access to the POP facilities is restricted to authorized personnel.	CC6.4
2.	Documented procedures exist for the identification and escalation of potential physical security breaches.	CC7.2
3.	Appropriate environmental controls such as air-conditioning, alternate power supply, fire extinguishers, and fire alarms are implemented, monitored, and maintained.	A1.2

User Entity Responsibilities

User entities must perform specific activities in order to benefit from US Signal's services. These activities may affect the user entity's ability to effectively use US Signal's services but do not affect the ability of US Signal to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and US Signal, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the system and are expected to be in operation at user entities to complement US Signal's controls. The list of

UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	User entities are responsible for ensuring that appropriate logical security controls are in place on their virtual servers at the operating system, application, database, and network levels.
2.	User entities are responsible for notifying US Signal Facilities Department of access changes to the data center facilities in a timely manner. User Organizations are also responsible for reviewing and approving access listings generated by US Signal Facilities Department on an annual basis.
3.	User entities are responsible for ensuring that identified problems are tracked and reported to the US Signal TOC, as required by the SLA, for tracking those problems.
4.	User entities are responsible for having controls in place to ensure that their data is backed up in a manner and frequency meeting User Organization needs.

IV. Trust Services Criteria, Applicable Requirements of the HIPAA Security Rule, Related Controls, Tests of Controls, and Results of Tests

Trust Services Criteria, Applicable Requirements of the HIPAA Security Rule, Related Controls, Tests of Controls, and Results of Tests

This report is intended to provide information to the management of US Signal, user entities of US Signal's network and data center services system, and prospective user entities, independent auditors, and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information, including information about the controls implemented by the user entities. This report is intended to provide information about the suitability of the design and operating effectiveness of controls implemented to achieve the service commitments and system requirements based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*, and the applicable administrative, physical, and technical safeguards as set forth in the Health Insurance Portability and Accountability Act (HIPAA), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308 316) (applicable requirements of the HIPAA security rule) throughout the period July 1, 2022 to June 30, 2023.

The examination was performed in accordance with attestation standards established by the AICPA, specifically, AT-C Sections 105 and 205 and the guidance contained in the AICPA Guide, *SOC 2 Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. It is each user entity's responsibility to evaluate this information in relation to its own system of internal control in order to assess its system of internal control. If an effective system of internal control is not in place at user entities, US Signal's controls may not compensate for such weaknesses.

This description is intended to focus on US Signal's controls surrounding the system throughout the period July 1, 2022 to June 30, 2023; it does not encompass all aspects of the services provided or controls performed by US Signal. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's system and the suitability of the design and operating effectiveness of controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule stated in the description, involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the

HIPAA security rule stated in the description were achieved throughout the period July 1, 2022 to June 30, 2023.

Our tests of controls were designed to cover a representative number of activities throughout the period July 1, 2022 to June 30, 2023 for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the applicable trust services criteria and the applicable requirements of the HIPAA security rule. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

BDO USA, P.C.'s testing of controls was restricted to the controls specified by US Signal in Section IV and was not extended to controls in effect at user entities or other controls that were not documented as tested under each control criteria listed in Section IV. The description of BDO USA, P.C.'s tests of controls and the results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of BDO USA, P.C. and should be considered information provided by BDO USA, P.C.

The basis for all tests of operating effectiveness includes inquiry of the individual(s) responsible for the control. As part of our testing of each control, we inquired of the individual(s) to determine the fairness of the description of the control and to evaluate the design and implementation of the control. As part of our inquiries, we also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, our inquiries were not listed individually for every control activity tested and shown in Section IV.

Additional testing of the control activities may have been performed using the following methods:

Method	Description
Inquiry	Inquired of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s), as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Presentation of Controls

Controls presented in the following tables may appear more than once if a control supports the achievement of multiple criteria. When a control is presented to support additional criteria, it will be presented with the original control number and after any new controls for those criteria.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
CC1.1	The entity demonstrates a commitment to integrity and ethical values. 164.316(b)(2)(ii) Documentation: Availability 164.308(b)(1) Business Associate Contracts and Other Arrangements	CC1.1.1	US Signal has a documented Business Conduct Policy within the Employee Handbook that defines employee conduct standards. The Employee Handbook is posted on the intranet and made available for employees to view.	Inspected the Employee Handbook to determine a Business Conduct Policy had been established to define employee conduct standards.	No exceptions noted.
				Inspected the intranet to determine the Employee Handbook had been made available to employees.	No exceptions noted.
		CC1.1.2	Employees are required to sign an acknowledgement stating they have read, understand, and agree to comply with the responsibilities and requirements outlined within the Employee Handbook and US Signal policies upon hire and annually thereafter.	Inspected acknowledgement forms of the Employee Handbook and US Signal policies for a selection of new hires to determine new hires were required to review and acknowledge the Employee Handbook and US Signal policies upon hire.	No exceptions noted.
				Inspected acknowledgement forms of the Employee Handbook and US Signal policies for a selection of current employees to determine employees were required to review and acknowledge the Employee Handbook and US Signal policies annually.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.1.3	Individuals offered positions at US Signal are subject to background checks as part of the employee screening process.	Inspected background check results for a selection of new hires to determine criminal background checks were completed as part of the employee screening process.	No exceptions noted.
		CC1.1.4	US Signal has an anonymous policy-violation complaint form available to internal users on the intranet. Compliance Management is automatically notified and monitors workforce member complaints reported via the form.	Inspected the intranet to determine the anonymous policy-violation complaint form was made available to internal users.	No exceptions noted.
				Inspected a test policy-violation complaint form and alert to determine Compliance Management was automatically notified and monitored workforce member complaints reported via the form.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	From July 1, 2022 through February 13, 2023, the Chairman, CEO, and Managing Member of US Signal was independent of the day-to-day operations of control owners and served in an oversight capacity of the line management overseeing those control owners.	Inspected the Board of Directors Statement to determine it established the responsibility of the Chairman, CEO, and Managing Member to provide oversight of line management and maintain independence from control owners.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.2.2	Beginning February 14, 2023, the roles and responsibilities of the US Signal Board of Directors are segregated from the roles and responsibilities of management. The Board is independent of the day-to-day operations of control owners and serves in an oversight capacity of the line management overseeing those control owners.	Inspected the Operating Agreement to determine the roles and responsibilities of the US Signal Board of Directors were segregated from the roles and responsibilities of management, and the Board was independent of the day-to-day operations of control owners.	No exceptions noted.
		CC1.2.3	From July 1, 2022 through February 13, 2023, the Chief Information Security Officer provided oversight of the development and performance of internal control through oversight of the Internal Audit Program and the Information Security Program, which drove the execution of US Signal's Governance, Risk, Compliance, and Security Program. The Chief Information Security Officer reported results directly to the Chairman, CEO, and Managing Member of US Signal.	Inspected the US Signal Internal Audit Charter and Information Security Program Charter to determine the Chief Information Security Officer was responsible for overseeing both charters.	No exceptions noted.
				Inspected the US Signal Internal Audit Charter to determine the Chief Information Security Officer was responsible for reporting results directly to the Chairman, CEO, and Managing Member of US Signal.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.2.4	Beginning February 14, 2023, the Chief Information Security Officer provides oversight of the development and performance of internal control through oversight of the Internal Audit Program and the Information Security Program, which drives the execution of US Signal's Governance, Risk, Compliance, and Security Program. The Chief Information Security Officer reports results directly to the Board of Directors of US Signal.	Inspected the US Signal Internal Audit Charter and Information Security Program Charter to determine the Chief Information Security Officer was responsible for overseeing both charters.	No exceptions noted.
				Inspected the Board of Directors meeting minutes to determine the Chief Information Security Officer was responsible for reporting results directly to the Board of Directors of US Signal.	No exceptions noted.
		CC1.2.5	Beginning February 14, 2023, the US Signal Board of Directors has established an audit subcommittee, which is responsible for oversight of the Internal Audit and Information Security Programs at US Signal.	Inspected the Board of Directors meeting minutes to determine the US Signal Board of Directors had established an audit subcommittee, which was responsible for oversight of the Internal Audit and Information Security Programs at US Signal.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. 164.308(a)(2) Assigned Security Responsibility	CC1.3.1	US Signal maintains an up-to-date organizational chart that outlines reporting lines and levels of authorities within the organization. The organizational chart is posted within the HR information system and made available for employees to view.	Inspected the US Signal organization chart to determine US Signal maintained an organization chart that outlined reporting lines and levels of authority.	No exceptions noted.
				Inspected the HR information system to determine the organization chart was posted and made available for employees to view.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.3.2	Roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description.	Inspected job descriptions for a selection of job titles to determine roles and responsibilities, as well as the knowledge and skills that are needed to perform them, were documented in written job descriptions.	No exceptions noted.
				Inspected employee qualification evaluations for a selection of new hires to determine each candidate's ability to meet required qualifications was evaluated during the hiring process.	No exceptions noted.
		CC1.3.3	The responsibility and accountability for updating and maintaining US Signal information security policies are assigned to the Chief Information Security Officer and executive leadership. US Signal policies are reviewed annually and updated as necessary.	Inspected the US Signal Information Security Policy to determine the Chief Information Security Officer and executive leadership were responsible and accountable for updating and maintaining information security policies.	No exceptions noted.
				Inspected US Signal information security policies to determine policies were reviewed and updated annually.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. 164.308(a)(5)(i) Security Awareness and Training 164.308(a)(5)(ii)(A) Security Awareness and Training: Security Reminders 164.308(a)(5)(ii)(B) Security Awareness and Training: Protection from Malicious Software 164.308(a)(5)(ii)(C) Security Awareness and Training: Log-in Monitoring 164.308(a)(5)(ii)(D) Security Awareness and Training: Password Management	CC1.4.1	On an at least annual basis, management performs people and resource planning to ensure appropriate staff and resources are available to meet the Company's objectives and presents to the Board of Directors for approval.	Inspected the annual budget to determine management performed people and resource planning to ensure appropriate staff and resources were available to meet the Company's objectives and presented to the Board of Directors for approval.	No exceptions noted.
		CC1.4.2	Employee performance is evaluated on an annual basis to determine that employees are qualified to fulfill their job responsibilities.	Inspected performance review results for a selection of current employees to determine employee performance was evaluated on an annual basis.	No exceptions noted.
		CC1.4.3	Employees are required to complete security awareness training when hired and on an annual basis thereafter.	Inspected the US Signal security training attendance log for a selection of new hires to determine new hires completed security awareness training upon hire.	No exceptions noted.
				Inspected the US Signal security training log for a selection of current employees to determine employees completed annual security awareness training.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		CC1.1.3	Individuals offered positions at US Signal are subject to background checks as part of the employee screening process.	Inspected background check results for a selection of new hires to determine criminal background checks were completed as part of the employee screening process.	No exceptions noted.
		CC1.3.2	Roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description.	Inspected job descriptions for a selection of job titles to determine roles and responsibilities, as well as the knowledge and skills that are needed to perform them, were documented in written job descriptions.	No exceptions noted.
				Inspected employee qualification evaluations for a selection of new hires to determine each candidate's ability to meet required qualifications was evaluated during the hiring process.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. 164.308(a)(1)(ii)(C) Security Management Process: Sanction Policy	CC1.5.1	US Signal has a documented Progressive Discipline Policy within the Employee Handbook, which is used to outline procedures around how they address conduct issues. When conduct issues occur, a discipline form is completed to document the issue and is signed by the employee, their supervisor, and HR.	Inspected the Employee Handbook to determine a Progressive Discipline Policy had been established.	No exceptions noted.
				A portion of the control did not operate during the examination period because no discipline issues were given during the examination period. Corroboratively inquired of the Vice President of HR and the Chief Information Security Officer to determine no discipline issues were given during the examination period.	Since the circumstances that warrant the operation of this portion of the control did not occur during the examination period, this portion of the control could not be tested.
		CC1.3.2	Roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description.	Inspected job descriptions for a selection of job titles to determine roles and responsibilities, as well as the knowledge and skills that are needed to perform them, were documented in written job descriptions.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
				Inspected employee qualification evaluations for a selection of new hires to determine each candidate's ability to meet required qualifications was evaluated during the hiring process.	No exceptions noted.
		CC1.3.3	The responsibility and accountability for updating and maintaining US Signal information security policies are assigned to the Chief Information Security Officer and executive leadership. US Signal policies are reviewed annually and updated as necessary.	Inspected the US Signal Information Security Policy to determine the Chief Information Security Officer and executive leadership were responsible and accountable for updating and maintaining information security policies.	No exceptions noted.
				Inspected US Signal information security policies to determine policies were reviewed and updated annually.	No exceptions noted.
		CC1.4.2	Employee performance is evaluated on an annual basis to determine that employees are qualified to fulfill their job responsibilities.	Inspected performance review results for a selection of current employees to determine employee performance was evaluated on an annual basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. 164.316(b)(1) Documentation 164.316(b)(2)(iii) Documentation: Updates 164.316(b)(2)(ii) Documentation: Availability	CC2.1.1	US Signal has implemented policies and procedures relevant to information security, and based on those policies and procedures, performs logical and physical security, change management, incident monitoring, and retention control activities, to ensure that the systems supporting the functioning of internal control are producing relevant, quality information.	Inspected the applicable policies and procedures to determine US Signal has implemented relevant information security policies and procedures.	No exceptions noted.
				Inspected the applicable IT general controls in place to determine US Signal's logical and physical security, change management, incident monitoring, and retention control activities are operating effectively to ensure that the systems supporting the functioning of internal control are producing relevant, quality information.	No exceptions noted.
		CC2.1.2	Descriptions of US Signal's systems are posted on the Company's intranet and are available to internal users to view. The descriptions delineate the boundaries of the systems and key aspects of processing.	Inspected the intranet to determine that descriptions of the systems were posted on the intranet and available to internal users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
				Inspected product specification documentation to determine descriptions of the systems were documented and delineated the boundaries of the system and key aspects of processing.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. 164.316(b)(1) Documentation 164.316(b)(2)(ii) Documentation: Availability	CC2.2.1	US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view.	Inspected the Incident Response Policy to determine the policy outlined steps that need to be taken when incidents are identified.	No exceptions noted.
				Inspected the intranet to determine the Incident Response Policy was posted on the entity's intranet and available to internal users.	No exceptions noted.
		CC2.2.2	US Signal has implemented formal customer support and incident management policies and procedures that document how customer service issues are handled. The policy is posted in the US Signal file directory and available for internal users to view.	Inspected the TOC maintenance overview document to determine that procedures had been established to address customer support issues.	No exceptions noted.
				Inspected the file directory to determine the TOC maintenance overview document was available for internal users to view.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
		CC2.2.3	US Signal maintains a system-change calendar that identifies and communicates planned changes throughout the year. It is posted and available for internal users to view through a shared MS Outlook calendar.	Inspected the MS Outlook calendar to determine the system-change calendar identified planned changes and was communicated to internal users.	No exceptions noted.
		CC2.2.4	System changes that affect US Signal services are communicated to applicable internal and external users as part of the implementation process.	Inspected the notification for a selection of system changes affecting US Signal services to determine system changes that affected US Signal services were communicated to applicable internal and external users.	No exceptions noted.
		CC1.1.2	Employees are required to sign an acknowledgement stating they have read, understand, and agree to comply with the responsibilities and requirements outlined within the Employee Handbook and US Signal policies upon hire and annually thereafter.	Inspected acknowledgement forms of the Employee Handbook and US Signal policies for a selection of new hires to determine new hires were required to review and acknowledge the Employee Handbook and US Signal policies upon hire.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
				Inspected acknowledgement forms of the Employee Handbook and US Signal policies for a selection of current employees to determine employees were required to review and acknowledge the Employee Handbook and US Signal policies annually.	No exceptions noted.
		CC1.4.3	Employees are required to complete security awareness training when hired and on an annual basis thereafter.	Inspected the US Signal security training attendance log for a selection of new hires to determine new hires completed security awareness training upon hire.	No exceptions noted.
				Inspected the US Signal security training log for a selection of current employees to determine employees completed annual security awareness training.	No exceptions noted.
		CC2.1.2	Descriptions of US Signal's systems are posted on the Company's intranet and are available to internal users to view. The descriptions delineate the boundaries of the systems and key aspects of processing.	Inspected the intranet to determine that descriptions of the systems were posted on the intranet and available to internal users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
				Inspected product specification documentation to determine descriptions of the systems were documented and delineated the boundaries of the system and key aspects of processing.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control. 164.308(b)(1) Business Associate Contracts and Other Arrangements 164.308(b)(4) Business Associate Contracts and Other Arrangements: Written Contract or Other Arrangement	CC2.3.1	System descriptions are available to external users through the customer portal that delineate the boundaries of the system and describe relevant components, as well as its purpose and design.	Inspected the customer portal to determine system descriptions were available to external users.	No exceptions noted.
				Inspected system descriptions to determine they were documented and delineated the boundaries of the system, as well as described relevant components and its purpose and design.	No exceptions noted.
		CC2.3.2	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected written agreements for a selection of new service providers and business partners to determine clearly defined terms, conditions, and responsibilities were included.	No exceptions noted.
		CC2.3.3	Products and services offered by US Signal have documented SLAs that are made available to customers on the US Signal website.	Inspected the US Signal website to determine SLAs for products and services offered by US Signal had been made available to customers.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
		CC2.3.4	US Signal's security, availability, and confidentiality responsibilities and commitments are communicated to external users within master agreements.	Inspected master agreement templates and example executed agreements to determine US Signal communicated their security, availability, and confidentiality responsibilities and commitments to external users.	No exceptions noted.
		CC2.3.5	Customers are provided information on how to report security events and service-related issues via phone, email, or through creating a trouble ticket through the customer portal to the TOC on the US Signal website.	Inspected the US Signal website to determine a published phone number and email address were available for customers to report security events and service-related issues.	No exceptions noted.
				Inspected the customer portal to determine customers were able to create a trouble ticket to report security events and service-related issues.	No exceptions noted.
		CC2.2.4	System changes that affect US Signal services are communicated to applicable internal and external users as part of the implementation process.	Inspected the notification for a selection of system changes affecting US Signal services to determine system changes that affected US Signal services were communicated to applicable internal and external users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. 164.308(a)(1)(i) Security Management Process	CC3.1.1	Management maintains a list of objectives and contractual commitments that is reviewed and updated on at least an annual basis to ensure that they are documented with sufficient clarity.	Inspected the list of objectives and contractual commitments to determine objectives and contractual commitments were documented with sufficient clarity and reviewed on at least an annual basis.	No exceptions noted.
		CC3.1.2	US Signal monitors service-level statistics on a quarterly basis to ensure that they are meeting company objectives. Results of the monitoring are communicated to management for review.	Inspected the service-level statistics for a selection of quarters to determine statistics and company objectives were monitored on a quarterly basis.	No exceptions noted.
				Inspected the meeting invite and agenda for a selection of quarters to determine service level statistics were communicated to management for review on a quarterly basis.	No exceptions noted.
		CC3.1.3	Management subscribes to external reporting services that identify changes to technology or regulations relating to services provided by US Signal.	Inspected email subscriptions to determine management subscribed to external reporting services that identify changes to technology or regulations relating to services provided by US Signal.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		CC3.1.4	The Information Security Team maintains an Information Security and Compliance road map that outlines the IT strategic objectives and projects. The road map is reviewed and updated by management on an at least annual basis.	Inspected the road map to determine the Information Security Team maintained an Information Security and Compliance road map that outlines the IT strategic objectives and projects. The road map was reviewed and updated by management on an at least annual basis.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. 164.308(a)(1)(i) Security Management Process 164.308(a)(1)(ii)(A) Security Management Process: Risk Analysis 164.308(a)(1)(ii)(B) Security Management Process: Risk Management 164.308(a)(8) Evaluation	CC3.2.1	US Signal performs a risk assessment over their environment on an annual basis to identify potential threats that would impair system security and availability and analyze the risk associated with the identified threats and determine mitigation strategies for those risks.	Inspected the US Signal risk assessment to determine it was completed on an annual basis and identified potential threats that would impair the system and potential mitigation strategies for those risks.	No exceptions noted.
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		CC3.2.3	US Signal has documented risks for each line of business to identify potential vulnerabilities and threats specific to each service they provide. The product-specific risk assessments are updated on an as-needed basis.	Inspected product-specific risk assessments to determine US Signal had documented potential vulnerabilities and threats specific to each service offering.	No exceptions noted.
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.3.1	As part of the annual risk assessment, management assesses fraud risk to identify the various ways that fraud and misconduct can occur within their environment, including how management might engage in inappropriate actions, and maintains documentation of this assessment.	Inspected the annual risk assessment to determine management contemplated fraud risk as part of the annual risk assessment and identified the various ways that fraud and misconduct may occur.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.4.1	US Signal, through its ongoing and annual risk-assessment process, evaluates changes in the regulatory and physical environment in which US Signal operates, as well as vendor and business-partner relationships.	Inspected the annual risk assessment to determine US Signal evaluated changes in the regulatory and physical environment in which US Signal operates, as well as vendor and business-partner relationships.	No exceptions noted.
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.
		CC3.1.3	Management subscribes to external reporting services that identify changes to technology or regulations relating to services provided by US Signal.	Inspected email subscriptions to determine management subscribed to external reporting services that identify changes to technology or regulations relating to services provided by US Signal.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.1	US Signal develops an audit schedule annually to assist with identifying and monitoring the various levels of risk within the organization.	Inspected the audit schedule to determine that US Signal had developed an audit plan annually.	No exceptions noted.
		CC4.1.2	Based on the audit schedule, US Signal performs various self-certification audits annually to test the design and operating effectiveness of controls within the environment. Audit reports are generated to document their procedures and results of the self-certification audits.	Inspected the audit reports for a selection of self-certification audits to determine that US Signal had performed audits to test the design and operating effectiveness of controls within the environment.	No exceptions noted.
		CC4.1.3	US Signal performs an internal assessment of their controls against the NIST CSF on at least an annual basis. Results of the assessment are reviewed by management to ensure that components of internal controls are present and functioning.	Inspected the internal NIST CSF assessment to determine that US Signal performed an assessment of their controls against the NIST CSF at least annually.	No exceptions noted.
				Inspected NIST CSF assessment to determine that management reviewed the annual NIST CSF assessment results.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Monitoring Activities					
		CC4.1.4	US Signal audits their data center facilities on an annual basis to ensure that the appropriate controls are in place and operating effectively at the facilities.	Inspected the audit reports for all US Signal data center facilities to determine that US Signal had performed an audit of their data center facilities on an annual basis.	No exceptions noted.
		CC3.1.2	US Signal monitors service-level statistics on a quarterly basis to ensure that they are meeting company objectives. Results of the monitoring are communicated to management for review.	Inspected the service-level statistics for a selection of quarters to determine statistics and company objectives were monitored on a quarterly basis by US Signal.	No exceptions noted.
				Inspected the meeting invite and agenda for a selection of quarters to determine service level statistics were communicated to management for review on a quarterly basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. 164.308(a)(8) Evaluation	CC4.2.1	The results of internal assessments are communicated to the CEO or executive leadership at least annually.	Inspected the email communication sent by internal audit to determine that results of internal assessments were communicated to CEO or executive leadership at least annually.	No exceptions noted.
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1	As part of its annual risk assessment, management links identified risks to controls that have been designed and implemented to address them.	Inspected the annual risk assessment to determine that management had linked identified risks to controls that were designed and implemented to address them.	No exceptions noted.
		CC4.1.3	US Signal performs an internal assessment of their controls against the NIST CSF on at least an annual basis. Results of the assessment are reviewed by Management to ensure that components of internal controls are present and functioning.	Inspected the internal NIST CSF assessment to determine that US Signal performed an assessment of their controls against the NIST CSF at least annually.	No exceptions noted.
				Inspected NIST CSF assessment to determine that Management reviewed the annual NIST CSF assessment results.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives. 164.310(d)(2)(iii) Device and Media Controls: Accountability	CC5.2.1	US Signal uses NIST as a framework to select and develop general control activities in the areas of security administration, application change control, systems development life cycle, and computer operations.	Inspected the internal NIST security framework assessment to determine that US Signal used NIST as their control framework.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
		CC5.2.2	US Signal selects logical and physical security, change management, and incident monitoring control activities to manage technology infrastructure and security access risks identified during the annual risk assessment process.	Inspected the logical and physical security, change management, and incident monitoring control activities to determine that controls were in place to manage technology infrastructure and security access risks identified during the annual risk assessment process.	No exceptions noted.
		CC5.2.3	From July 1, 2022 through February 13, 2023, US Signal monitors their asset inventory via their Information Security and Compliance scorecard. The scorecard is updated and reviewed as part of the monthly Executive Security Team meetings.	Inspected the Information Security and Compliance scorecard for a selection of months to determine that US Signal monitored their asset inventory on a monthly basis.	No exceptions noted.
				Inspected the Executive Security Team meeting minutes to determine that the scorecard was updated and reviewed as part of the Executive Security Team meeting.	No exceptions noted.
		CC5.2.4	Beginning February 14, 2023, on a quarterly basis, US Signal monitors their asset inventory and results are reported to management for review.	Inspected meeting minutes for a selection of quarters to determine that the US Signal monitored their asset inventory and results were reported to management for review.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
		CC5.1.1	As part of its annual risk assessment, management links identified risks to controls that have been designed and implemented to address them.	Inspected the annual risk assessment to determine that management had linked identified risks to controls that were designed and implemented to address them.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. 164.316(a) Policies and Procedures 164.316(b)(1) Documentation 164.316(b)(2)(ii) Documentation: Availability 164.316(b)(2)(iii) Documentation: Updates	CC1.3.2	Roles and responsibilities, as well as the knowledge and skills that are needed to perform them, are defined in written job descriptions. During the hiring process, management reviews job descriptions to ensure that the candidates possess the required qualifications to perform the duties outlined in the job description.	Inspected job descriptions for a selection of job titles to determine roles and responsibilities, as well as the knowledge and skills that are needed to perform them, were documented in written job descriptions.	No exceptions noted.
				Inspected employee qualification evaluations for a selection of new hires to determine each candidate's ability to meet required qualifications was evaluated during the hiring process.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
		CC1.3.3	The responsibility and accountability for updating and maintaining US Signal information security policies are assigned to the Chief Information Security Officer and executive leadership. US Signal policies are reviewed annually and updated as necessary.	Inspected the US Signal Information Security Policy to determine the Chief Information Security Officer and executive leadership were responsible and accountable for updating and maintaining information security policies.	No exceptions noted.
				Inspected US Signal information security policies to determine policies were reviewed and updated annually.	No exceptions noted.
		CC2.1.1	US Signal has implemented policies and procedures relevant to information security, and based on those policies and procedures, performs logical and physical security, change management, incident monitoring, and retention control activities, to ensure that the systems supporting the functioning of internal control are producing relevant, quality information.	Inspected the applicable policies and procedures to determine US Signal has implemented relevant information security policies and procedures.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
				Inspected the applicable IT general controls in place to determine US Signal's logical and physical security, change management, incident monitoring, and retention control activities are operating effectively to ensure that the systems supporting the functioning of internal control are producing relevant, quality information.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. 164.308(a)(3)(i) Workforce Security 164.308(a)(5)(ii)(D) Security Awareness and Training: Password Management 164.312(a)(1) Access Control 164.312(a)(2)(i) Access Control: Unique User Identification 164.312(a)(2)(iii) Access Control: Automatic Logoff 164.312(d) Person or Entity Authentication 164.312(c)(2) Mechanism to Authenticate Electronic	CC6.1.1	Customer data storage is segregated into individual virtual storage repositories so that customers do not have access to other customers' data.	Inspected the virtual storage dashboard and the cloud customer storage diagram to determine that access to customer data was segregated.	No exceptions noted.
		CC6.1.2	US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	Inspected a network diagram and firewall configurations to determine that firewalls had been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	No exceptions noted.
		CC6.1.3	Firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats.	Inspected firewall security settings and the logging tool used by US Signal to determine that firewall performance was monitored.	No exceptions noted.
				Inspected firewall system settings and the logging tool used by US Signal to determine that intrusion prevention would detect and alert system administrators to potential threats.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CC6.1.4	Access to the individual production network elements and managed CPE is authenticated through a centralized RADIUS server.	Inspected security configurations for production network elements and managed CPE to determine that access to the devices was controlled through a centralized RADIUS server.	No exceptions noted.
		CC6.1.5	Access to production network elements is configured to be restricted to specific protocols, ports, and IP addresses.	Inspected the configuration of production network elements to determine that access was configured to be restricted to specific protocols, ports, and IP addresses.	No exceptions noted.
		CC6.1.6	Access to the RADIUS server, which restricts access to the production network elements, is configured to authenticate via Active Directory.	Inspected RADIUS server configurations to determine it was configured to authenticate via Active Directory.	No exceptions noted.
		CC6.1.7	In accordance with the US Signal Information Security Policy, users with access to US Signal systems require a uniquely assigned identifiable user ID.	Inspected the Information Security Policy to determine that it documented the requirement for users needing unique user IDs to access US Signal systems.	No exceptions noted.
				Inspected the list of network users for the US Signal domain to determine that users were assigned unique user IDs.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
				Inspected the list of OMNI users to determine that users were assigned unique user IDs.	No exceptions noted.
		CC6.1.8	Network password restrictions are enabled for password length, strength, duration, history, and lockout settings.	Inspected the default password and lockout policies for the US Signal domain to determine that passwords were enabled and enforced password length, strength, duration, history, and account lockout.	No exceptions noted.
		CC6.1.9	OMNI password parameters are in place and are set to require minimum length, complexity, expiration, history, and lockout settings.	Inspected the OMNI password parameters to determine that it was configured to enforce minimum length, complexity, expiration, history, and lockout settings.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. 164.308(a)(3)(ii)(A) Workforce Security: Authorization and/or Supervision 164.308(a)(3)(ii)(B) Workforce Security: Workforce Clearance 164.308(a)(3)(ii)(C) Workforce Security: Termination 164.308(a)(4)(i) Information Access Management	CC6.2.1	HR personnel or Department Managers submit requests for access to the production network elements to the IT Helpdesk who validate the request was properly authorized and configure access in the production (RADIUS) server.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the production network to determine that the access was approved by HR personnel or the employee's Department Manager	No exceptions noted.
				Inspected the access in the RADIUS server for a selection of new hires granted access to the production network to determine that the access was appropriately granted based on the user's role and as requested.	No exceptions noted.
		CC6.2.2	HR personnel or Department Managers submit requests for new-user access to the domain to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates the new user's accounts with the appropriate access based on the user's role and access requested.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the domain to determine that the access was approved by HR personnel or the employee's Department Manager.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
	164.308(a)(4)(ii)(B) Information Access Management: Access Authorization 164.308(a)(4)(ii)(C) Information Access Management: Access Establishment and Modification 164.312(a)(1) Access Control			Inspected the access in the US Signal domain for a selection of new hires granted access to the domain to determine that the access was appropriately granted based on the user's role and access requested.	No exceptions noted.
		CC6.2.3	HR personnel or Department Managers submit requests for new user access to the OMNI application to the IT Helpdesk through an email or ticket. The IT Helpdesk Analyst validates the request and creates or modifies the user's account with the appropriate access based on the user's role and access requested.	Inspected the email or IT Helpdesk ticket for a selection of new hires granted access to the OMNI application to determine that access was approved by HR personnel or the employee's Department Manager.	No exceptions noted.
				Inspected the OMNI application user listing for a selection of new hires granted access to the OMNI application to determine that access was appropriately granted based on the user's role and access requested.	No exceptions noted.
		CC6.2.4	Upon employee termination, the IT Helpdesk removes access to US Signal systems after being notified of the termination by HR personnel.	Inspected the termination notification for a selection of terminated employees to determine that HR personnel notified the IT Helpdesk of the termination.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
				Inspected the domain user listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
				Inspected the OMNI listing for a selection of terminated employees to determine that access was removed.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. 164.308(a)(1)(ii)(D) Security Management Process: Information System Activity Review 164.308(a)(3)(i) Workforce Security	CC6.3.1	Users with the ability to access the vSphere are limited to authorized and appropriate IT personnel based on job responsibilities.	Inspected the access listing for the vSphere to determine that access was limited to appropriate IT personnel based on job responsibilities.	No exceptions noted.
				Corroboratively inquired of the Director of Technical Operations and Director of Information Security to determine that access to create or modify users was limited to authorized and appropriate IT personnel based on their job responsibilities.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
	164.308(a)(3)(ii)(A) Workforce Security: Authorization and/or Supervision 164.308(a)(3)(ii)(B) Workforce Security: Workforce Clearance 164.308(a)(3)(ii)(C) Workforce Security: Termination 164.308(a)(4)(i) Information Access Management 164.308(a)(4)(ii)(B) Information Access Management: Access Authorization 164.308(a)(4)(ii)(C) Information Access Management: Access Establishment and Modification 164.312(a)(1) Access Control	CC6.3.2	The ability to create or modify users and user access privileges is limited to authorized and appropriate IT personnel based on job responsibilities.	Inspected the listing of users with administrative access to the domain to determine that access was restricted to appropriate IT personnel based on job responsibilities.	No exceptions noted.
				Corroboratively inquired of the Director of Technical Operations and Director of Information Security to determine that access to create or modify users was limited to authorized and appropriate IT personnel based on their job responsibilities.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CC6.3.3	Privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems is reviewed by management on a quarterly basis to ensure that privileged access is restricted to appropriate users based on their job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the privileged access reviews for a selection of quarters to determine that privileged access to the network, applications, application databases, secured network drives, and back-end supporting systems were reviewed to ensure that privileged access was restricted to appropriate users based on their job responsibilities, and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.
		CC6.3.4	User access to the network is reviewed on a quarterly basis by management to ensure that access is restricted to appropriate users based on job responsibilities. Any access modifications needed as a result of the review are made by management.	Inspected the network access reviews for a selection of quarters to determine that user access to the network was reviewed by management for appropriateness and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. 164.310(a)(1) Facility Access Controls 164.310(a)(2)(ii) Facility Access Controls: Facility Security Plan 164.310(a)(2)(iii) Facility Access Controls: Access Control and Validation Procedures 164.310(c) Workstation Security	CC6.4.1	Access to the corporate headquarters and data center facilities containing production servers and telecommunication equipment is controlled and restricted by an electronic proximity card or biometric access system.	For the corporate headquarters and each US Signal data center facility, observed the proximity card access or biometric access system in place to determine that access to the facility was controlled and restricted from unauthorized access by an electronic proximity card or biometric access system.	No exceptions noted.
		CC6.4.2	The data center facilities' camera and alarm systems are monitored on an ongoing basis by the TOC. Camera and alarm systems are in place at each data center facility to ensure each location is secured and monitored.	Observed the TOC personnel performing their normal duties to determine that US Signal data center facility's cameras and alarm systems were monitored on an ongoing basis.	No exceptions noted.
				For each US Signal data center facility, observed the cameras and security alarm to determine that the data centers were secured and monitored.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CC6.4.3	For employees, requests for new access or changes to existing access are submitted to the Facilities Department from HR personnel. For customers and vendors, requests for new access or changes to existing access are submitted to the Facilities Department from the customer's or vendor's designated point of contact. The Facilities Manager validates the request and creates the new user's access based on the request.	Inspected the email notification sent to the Facilities Department and a ticket for a selection of employees, customers, and vendors who were granted new facilities access or had a change to their existing facilities access to determine that requests for new access or changes to existing access were authorized prior to access being granted.	No exceptions noted.
		CC6.4.4	When employees leave the organization, HR personnel reclaim the terminated employee's access card and notify the Facilities Manager via email or ticket so that physical access privileges, such as biometrics or proximity card, will be revoked.	Inspected the email or ticket notification for a selection of terminated employees to determine that HR personnel had notified facilities to disable or revoke physical access.	No exceptions noted.
				Inspected the facilities' physical access listing for a selection of terminated employees to determine that physical access was revoked.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CC6.4.5	When US Signal receives a request for removal of customer access to the data center, a ticket is created to track the removal of physical access.	Inspected customer facilities tickets for a selection of customer removal requests to determine access was removed appropriately and physical access removal was tracked in a ticket.	No exceptions noted.
		CC6.4.6	Physical access to the corporate headquarters and data center facilities is reviewed on a quarterly basis by management. Any access modifications needed as a result of the review are made by management.	Inspected the physical access reviews for a selection of quarters to determine that physical access to the corporate headquarters and data center facilities was reviewed by management and any access modifications as a result of the review were made by management, if needed.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. 164.310(d)(1) Device and Media Controls 164.310(d)(2)(i) Device and Media Controls: Disposal 164.310(d)(2)(ii) Device and Media Controls: Media Reuse	CC6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the Data Protection Policy and the Data Sanitization Policy to determine that formal data retention and disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
		CC6.5.2	Equipment potentially storing digital media is degaussed, sanitized, and/or securely destroyed prior to the equipment being removed from the US Signal facility or data centers.	Inspected the erasure log output for a selection of equipment removed from the US Signal facility or data centers to determine that equipment potentially storing digital media was degaussed, sanitized, and/or securely destroyed prior to the equipment being removed from the US Signal facility or data centers.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries. 164.308(a)(1)(i) Security Management Process	CC6.6.1	The US Signal production network elements are managed via an out-of-band network that is segregated from the carrier transport network to ensure separation of the management and production network.	Inspected the network diagram to determine that production network elements were managed via an out-of-band network that was segregated from the carrier transport network.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
	164.308(a)(1)(ii)(B) Security Management Process: Risk Management 164.312(e)(1) Transmission Security 164.312(c)(2) Mechanism to Authenticate Electronic	CC6.6.2	Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo security two-factor authentication connectivity.	Inspected Microsoft Duo configurations to determine that two-factor authentication was used by Active Directory users connecting to the network remotely.	No exceptions noted.
		CC6.1.2	US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	Inspected a network diagram and firewall configurations to determine that firewalls had been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	No exceptions noted.
		CC6.1.3	Firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats.	Inspected firewall security settings and the logging tool used by US Signal to determine that firewall performance was monitored.	No exceptions noted.
				Inspected firewall system settings and the logging tool used by US Signal to determine that intrusion prevention would detect and alert system administrators to potential threats.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. 164.308(a)(1)(i) Security Management Process 164.312(a)(2)(iv) Access Control: Encryption and Decryption 164.312(e)(1) Transmission Security 164.312(e)(2)(i) Transmission Security: Integrity Controls 164.312(e)(2)(ii) Transmission Security: Encryption and Decryption	CC6.7.1	US Signal uses WPA2 encryption on wireless network connections, and access is limited to Active Directory users.	Inspected wireless security configurations to determine that WPA2 encryption was used on wireless network connections and that access was restricted to Active Directory users.	No exceptions noted.
		CC6.7.2	US Signal's Information Security Policy prohibits the transmission of sensitive information over the internet or other public communications paths (for example, email), unless it is encrypted.	Inspected the Information Security Policy to determine that it documented the requirement to encrypt data transmitted over insecure channels.	No exceptions noted.
				Inspected configuration settings to determine that data transmitted over the internet or other public communication paths was encrypted.	No exceptions noted.
		CC6.7.3	DLP software scans for sensitive information in outgoing transmissions over public communication paths. Information that is restricted is blocked from outgoing transmissions.	Inspected the DLP software to determine that the software was configured to scan for sensitive information in outgoing transmissions over public communication paths.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
	164.310(b) Workstation Use 164.312 (e) (2)(ii) Encryption and Decryption	CC6.7.4	Storage for workstations and laptops is encrypted at rest via BitLocker.	Inspected BitLocker for a selection of workstations and laptops to determine that information in storage was encrypted at rest.	No exceptions noted.
		CC6.7.5	Removable media for workstations and laptops are also encrypted automatically by the software.	Inspected checkpoint endpoint-security software configurations to determine that they were in place on workstations and laptops to automatically encrypt removable media.	No exceptions noted.
		CC6.6.2	Remote access to the US Signal internal network is permitted for Active Directory users via VPN connectivity with Duo security two-factor authentication connectivity.	Inspected Microsoft Duo configurations to determine that two-factor authentication was used by Active Directory users connecting to the network remotely.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. 164.308(a)(1)(i) Security Management Process	CC6.8.1	Antivirus software protects production and email servers, workstations, and network-connected laptops against viruses and other malicious code.	Inspected the antivirus software for a selection of workstations and network-connected laptops to determine that antivirus software had been installed.	No exceptions noted.
				Inspected the antivirus software for a selection of servers to determine that antivirus software had been installed.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
	164.308(a)(1)(ii)(B) Security Management Process: Risk Management 164.308(a)(5)(ii)(B) Security Awareness and Training: Protection from Malicious Software	CC6.8.2	Antivirus software is configured to monitor data and traffic on production and email servers, workstations, and network-connected laptops with virus signature definitions that are automatically updated from the vendor.	Inspected the antivirus software configurations to determine that it was configured to monitor data and traffic on production and email servers, workstations, and network-connected laptops with virus signature definitions that are automatically updated from the vendor.	No exceptions noted.
		CC6.8.3	US Signal has a predefined listing of software that is prohibited from being installed on company laptops and workstations. Software on the predefined listing is automatically uninstalled, and IT is alerted.	Inspected the list of predefined prohibited software to determine that IT had a predefined list in place.	No exceptions noted.
				Inspected ManageEngine configurations to determine that it was configured to uninstall software on the predefined listing and alert IT.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. 164.308(a)(1)(ii)(A) Security Management Process: Risk Analysis 164.308(a)(1)(ii)(D) Security Management Process: Information System Activity Review	CC7.1.1	Internal and external vulnerability scans are performed on at least a quarterly basis, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements. Vulnerabilities identified from the scans are reviewed by management to ensure that they are being tracked and resolved in a timely manner.	Inspected internal and external vulnerability scans for a selection of quarters to determine scans were being performed on at least a quarterly basis.	No exceptions noted.
				Inspected a meeting invite to determine vulnerabilities identified were reviewed during the meeting to ensure that they were being tracked and resolved.	No exceptions noted.
		CC7.1.2	A network segmentation test is performed on an annual basis and identified failures from the test will result in a finding within the report. If failures are identified from the test, the Information Security Team will further investigate and resolve the issue.	Inspected the network segmentation test report to determine network segmentation testing was performed on an annual basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
				A portion of the control did not operate during the examination period because there were no failures identified from the test that required resolution during the examination period. Corroboratively inquired of the Director of Information Technology and the Chief Information Security Officer to determine there were no failures identified from the test that required resolution during the examination period.	Since the circumstances that warrant the operation of this portion of the control did not occur during the examination period, this portion of the control could not be tested.
		CC7.1.3	Penetration testing is performed on an annual basis. Critical and high-risk findings identified from the tests are tracked and resolved.	Inspected the annual penetration testing results to determine management performed the tests annually.	No exceptions noted.
				Inspected tickets for a selection of critical and high-risk findings from the annual penetration testing to determine management followed up on critical and high-risk findings for resolution.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC7.1.4	Logging and monitoring of security events are enabled on network elements and are configured to log activity to an internal SIEM and the Company's NMS.	Inspected configurations of production network elements for a selection of devices to determine they were configured to log activity to the internal SIEM and NMS.	No exceptions noted.
		CC7.1.5	Potential Active Directory security violations, including users gaining administrative access to the system, are logged within the SIEM.	Inspected InsightIDR logs to determine potential Active Directory security violations were logged within the SIEM.	No exceptions noted.
		CC7.1.6	Security events from the NMS are monitored in real time by the TOC.	Observed TOC personnel to determine they monitored security events in real time through the NMS.	No exceptions noted.
		CC7.1.7	System firewall audits are conducted on at least a biannual basis to validate firewall configurations are appropriate.	Inspected email communications and firewall change tickets to determine system firewall audits were conducted on at least a biannual basis to validate firewall configurations were appropriate.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC6.1.2	US Signal has firewalls at the perimeter of their network to protect their corporate systems from external threats. These firewalls have been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	Inspected a network diagram and firewall configurations to determine that firewalls had been configured to protect the perimeter connection, interconnections with customers' networks, and secure network entry points within the organization.	No exceptions noted.
		CC6.1.3	Firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats.	Inspected firewall security settings and the logging tool used by US Signal to determine that firewall performance was monitored.	No exceptions noted.
				Inspected firewall system settings and the logging tool used by US Signal to determine that intrusion prevention would detect and alert system administrators to potential threats.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. 164.312(b) Audit Controls	CC6.1.3	Firewalls include intrusion prevention features to detect and alert on potential threats. Specific thresholds are defined within the IDS/IPS tools, and a breach of those thresholds automatically sends logs to a log aggregation tool and alerts US Signal of potential threats.	Inspected firewall security settings and the logging tool used by US Signal to determine that firewall performance was monitored.	No exceptions noted.
				Inspected firewall system settings and the logging tool used by US Signal to determine that intrusion prevention would detect and alert system administrators to potential threats.	No exceptions noted.
		CC7.1.1	Internal and external vulnerability scans are performed on at least a quarterly basis, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements. Vulnerabilities identified from the scans are reviewed by management to ensure that they are being tracked and resolved in a timely manner.	Inspected internal and external vulnerability scans for a selection of quarters to determine scans were being performed on at least a quarterly basis.	No exceptions noted.
				Inspected a meeting invite to determine vulnerabilities identified were reviewed during the meeting to ensure that they were being tracked and resolved.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC7.1.2	A network segmentation test is performed on an annual basis and identified failures from the test will result in a finding within the report. If failures are identified from the test, the Information Security Team will further investigate and resolve the issue.	Inspected the network segmentation test report to determine network segmentation testing was performed on an annual basis.	No exceptions noted.
				A portion of the control did not operate during the examination period because there were no failures identified from the test that required resolution during the examination period. Corroboratively inquired of the Director of Information Technology and the Chief Information Security Officer to determine there were no failures identified from the test that required resolution during the examination period.	Since the circumstances that warrant the operation of this portion of the control did not occur during the examination period, this portion of the control could not be tested.
		CC7.1.3	Penetration testing is performed on an annual basis. Critical and high-risk findings identified from the tests are tracked and resolved.	Inspected the annual penetration testing results to determine management performed the tests annually.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
				Inspected tickets for a selection of critical and high-risk findings from the annual penetration testing to determine management followed up on critical and high-risk findings for resolution.	No exceptions noted.
		CC7.1.4	Logging and monitoring of security events are enabled on network elements and are configured to log activity to an internal SIEM and the Company's NMS.	Inspected configurations of production network elements for a selection of devices to determine they were configured to log activity to the internal SIEM and NMS.	No exceptions noted.
		CC7.1.5	Potential Active Directory security violations, including users gaining administrative access to the system, are logged within the SIEM.	Inspected InsightIDR logs to determine potential Active Directory security violations were logged within the SIEM.	No exceptions noted.
		CC7.1.6	Security events from the NMS are monitored in real time by the TOC.	Observed TOC personnel to determine they monitored security events in real time through the NMS.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. 164.308(a)(5)(ii)(C) Security Awareness and Training: Log-in Monitoring 164.308(a)(6)(i) Security Incident Procedures 164.308(a)(6)(ii) Security Incident Procedures: Response and Reporting 164.312(b) Audit Controls	CC7.3.1	TOC personnel document service issues that have been identified and reported to them through the NMS or by internal and external users within a ticketing system. TOC personnel review the issue and close a ticket once the item has been addressed.	Inspected the TOC ticket for a selection of service issues identified and reported to the TOC to determine TOC personnel reviewed the issue and closed the ticket once the item had been addressed.	No exceptions noted.
		CC7.3.2	Security events are documented within Service Cloud tickets. Security Operations Center personnel review Service Cloud tickets to determine if the events have been resolved, or if they need to be investigated further as an incident.	Inspected the Security Operations Center ticket for a selection of security events to determine Service Cloud tickets were created to document security events and the tickets were reviewed and addressed by Security Operations Center personnel.	No exceptions noted.
		CC2.2.1	US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view.	Inspected the Incident Response Policy to determine the policy outlined steps that need to be taken when incidents are identified.	No exceptions noted.
				Inspected the intranet to determine the Incident Response Policy was posted on the entity's intranet and available to internal users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC7.1.6	Security events from the NMS are monitored in real time by the TOC.	Observed TOC personnel to determine they monitored security events in real time through the NMS.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. 164.308(a)(6)(i) Security Incident Procedures 164.308(a)(6)(ii) Security Incident Procedures: Response and Reporting	CC7.4.1	Identified security, availability, or confidentiality incidents are documented and tracked within incident response reports. US Signal researches the potential impact of the identified incident and documents how it was resolved within the report.	Control did not operate during the examination period because there were no incidents relating to security, availability, or confidentiality that occurred within the examination period. Inspected the incident query to determine there were no incidents relating to security, availability, or confidentiality that occurred during the examination period.	Since the circumstances that warrant the operation of the control did not occur within the examination period, the control could not be tested.
		CC2.2.1	US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view.	Inspected the Incident Response Policy to determine the policy outlined steps that need to be taken when incidents are identified.	No exceptions noted.
				Inspected the intranet to determine the Incident Response Policy was posted on the entity's intranet and available to internal users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents. 164.308(a)(6)(i) Security Incident Procedures 164.308(a)(6)(ii) Security Incident Procedures: Response and Reporting	CC7.5.1	After an incident has been mitigated or resolved, a root-cause analysis of the incident is performed to ensure that the appropriate activities are implemented to recover from the incident.	Control did not operate during the examination period because there were no incidents relating to security, availability, or confidentiality that occurred within the examination period. Inspected the incident query to determine there were no incidents relating to security, availability, or confidentiality that occurred during examination period.	Since the circumstances that warrant the operation of the control did not occur within the examination period, the control could not be tested.
		CC7.5.2	Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure that the incident response procedures are up to date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents.	Inspected evidence of annual testing of the incident response plan to determine it was performed, that they were up to date and accurate, and that lessons learned as a result of the exercise were documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC2.2.1	US Signal has developed an Incident Response Policy that outlines steps that need to be taken when incidents are identified. The policy is posted online and available for internal users to view.	Inspected the Incident Response Policy to determine the policy outlined steps that need to be taken when incidents are identified.	No exceptions noted.
				Inspected the intranet to determine the Incident Response Policy was posted on the entity's intranet and available to internal users.	No exceptions noted.
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. 164.310(b) Workstation Use	CC8.1.1	US Signal has a formalized Data Protection Policy posted on their intranet to guide personnel in the design, testing, and implementation of systems.	Inspected the Data Protection Policy to determine that formalized procedures existed to guide personnel in the design, testing, and implementation of systems.	No exceptions noted.
				Inspected the US Signal intranet to determine that the Data Protection Policy was posted and available for internal personnel.	No exceptions noted.
		CC8.1.2	Development/staging environments are separated from production environments.	Inspected server configurations to determine that the development/ staging environments were separate from the production environment.	No exceptions noted.
		CC8.1.3	Management meets on a weekly basis to review and discuss past, in-progress, and upcoming changes, as well as current project status and development statistics.	Inspected meeting minutes for a selection of weeks to determine that management met on a weekly basis to discuss past, in-progress, and upcoming changes, as well as current project status and development statistics.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
		CC8.1.4	Requests to implement new or change existing customer equipment are documented within project checklists, where a project manager verifies the appropriate steps are completed based on the type of request, including testing and authorization by the customer.	Inspected project manager checklists and supporting documentation for a selection of orders for new customer equipment or changes to existing customer equipment to determine that a project manager completed the checklist and documented the completion of the appropriate steps for the order.	No exceptions noted.
		CC8.1.5	Changes to US Signal's internal infrastructure are documented within tickets and approved prior to the change being made.	Inspected tickets for a selection of infrastructure changes to determine that the change was documented within a ticket and approved prior to the change being made.	No exceptions noted.
		CC8.1.6	Project changes are requested by the business via email or a ticket. Once requested and approved, the project is documented and logged into the backlog to begin development.	Inspected emails or tickets and the development backlog for a selection of projects to determine that project changes were requested by the business and approved by placing it onto the backlog.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
		CC8.1.7	Project code changes are reviewed by a peer programmer who was not responsible for the change prior to the change being deployed to production.	Inspected GitHub pull requests for a selection of projects to determine that project code changes were reviewed by a peer programmer who was not responsible for the change prior to the change being placed into production.	No exceptions noted.
		CC8.1.8	Project changes are tested by the business prior to the change being implemented into production.	Inspected emails for a selection of projects to determine that project changes were tested by the business prior to the change being implemented into production.	No exceptions noted.
		CC8.1.9	Minor/emergency code changes are documented within tickets and reviewed by a peer programmer who was not responsible for the change prior to the change being placed into production.	Inspected tickets for a selection of minor/emergency code changes to determine that they were documented within tickets.	No exceptions noted.
				Inspected GitHub pull requests for a selection of minor/emergency code changes to determine that they were reviewed by a peer programmer who was not responsible for the change prior to the change being placed into production.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
		CC8.1.10	Access to deploy changes to production is limited to appropriate users and segregated from access to development, except for two select users who require access to both environments in order to support customer requests. Where access is required to both environments, changes to source code made by those users require a secondary review and approval prior to the code being deployed.	Inspected the listing of users with access to deploy changes into production to determine that access was limited to appropriate users and segregated from access to development, except for two select users.	No exceptions noted.
				Inspected the GitHub branch protection rule configurations to determine it was configured to require a secondary review and approval prior to merging code into the master branch.	No exceptions noted.
		CC8.1.11	Notifications are configured within GitHub to alert the US Signal software development team of and changes that are made.	Inspected GitHub notification configurations to determine it was configured notify personnel of changes being merged for production.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
		CC8.1.12	Beginning January 9, 2023, logging and monitoring of Github are configured to log activity to an internal SIEM. Any Github changes that require investigation are documented within event tickets. Security Operations Center personnel review tickets to determine if the events have been resolved, or if they need to be investigated further as an incident.	Inspected Github monitoring configurations to determine it was configured to log activity to the internal SIEM.	No exceptions noted.
				Inspected a user listing of users with access to modify the Github monitoring configurations to determine that access was limited to appropriate users and was segregated from access to development and production.	No exceptions noted.
				Inspected the Security Operations Center ticket for a selection of security events to determine tickets were created to document security events and the tickets were reviewed by Security Operations Center personnel.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Mitigation					
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. 164.308(a)(8) Evaluation 164.308(a)(7)(i) Contingency Plan 164.308(a)(7)(ii)(C) Contingency Plan: Emergency Mode Operation 164.310(a)(2)(i) Facility Access Controls: Contingency Operations	CC9.1.1	US Signal has developed a risk-management program. The risk-management program includes the use of insurance to minimize the financial impact of any loss events.	Inspected the certificate of liability insurance to determine US Signal maintained insurance to offset the financial impact of loss events that would impair the ability of US Signal to meet its objectives.	No exceptions noted.
		CC1.2.6	Beginning February 14, 2023, the Board of Directors and subcommittees meet to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	Inspected the Board of Directors meeting minutes for a selection of quarters to determine the Board of Directors and subcommittees met to discuss and monitor progress in the areas of audit, compensation, governance, risk, strategy, and other topics as needed on at least a quarterly basis.	No exceptions noted.
		CC3.2.1	US Signal performs a risk assessment over their environment on an annual basis to identify potential threats that would impair system security and availability and analyze the risk associated with the identified threats and determine mitigation strategies for those risks.	Inspected the US Signal risk assessment to determine it was completed on an annual basis and identified potential threats that would impair the system and potential mitigation strategies for those risks.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Mitigation					
		CC3.2.2	From July 1, 2022 through February 13, 2023, the Executive Security Team met monthly to review the results of operations, audits, and to discuss the risk assessment, including identifying new risks and developing and implementing appropriate measures to address new risks.	Inspected Executive Security Team meeting minutes for a selection of months to determine operations, audits, and risk assessment results were reviewed by the Executive Security Team.	No exceptions noted.
		A1.2.8	A Business Continuity and Disaster Recovery Manual has been established, and the manual is reviewed and tested at least annually.	Inspected the US Signal Business Continuity and Disaster Recovery Manual to determine that a manual had been established and was reviewed at least annually.	No exceptions noted.
				Inspected the Business Continuity and Disaster Recovery Summary document to determine that disaster recovery and business continuity tests were performed on an annual basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality, and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Mitigation					
CC9.2	The entity assesses and manages risks associated with vendors and business partners. 164.308(b)(1) Business Associate Contracts and Other Arrangements 164.308(b)(4) Business Associate Contracts and Other Arrangements: Written Contract or Other Arrangement	CC9.2.1	US Signal has a documented Vendor Management Policy that outlines their vendor due-diligence procedures. Based on the policy, US Signal performs annual due diligence on high-risk vendors to ensure that the risk associated with vendors is managed.	Inspected the Vendor Management Policy to determine it documented US Signal's vendor due-diligence procedures.	No exceptions noted.
				Inspected the vendor assessment for a selection of high-risk vendors to determine US Signal performed annual due diligence on high-risk vendors.	No exceptions noted.
		CC2.3.2	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected written agreements for a selection of new service providers and business partners to determine clearly defined terms, conditions, and responsibilities were included.	No exceptions noted.

Additional Criteria Related to Availability and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A1.1.1	US Signal's equipment that monitors managed CPE is configured to log and trap link status to the NMS. If a managed CPE does not communicate to the monitoring equipment, the link status of the CPE is logged in the NMS, and the TOC receives the underlying Managed Service Alarm(s) and responds in accordance with established policies and procedures to ensure that the stated SLA for the service is provided.	Inspected the NMS dashboards to determine that CPE log and trap link status was configured to be monitored within the NMS.	No exceptions noted.
				Inspected the NMS alarm board to determine that TOC personnel received alarms when CPE did not communicate to the monitoring equipment.	No exceptions noted.
				Inspected the TOC ticket for a selection of alarms received through the NMS to determine that TOC personnel responded to the alarm.	No exceptions noted.
		A1.1.2	Managed data center physical hardware, software, and network elements are configured to be monitored for availability using the NMS. The NMS has been configured to alert TOC staff in the event that a piece of physical hardware, software, or element becomes unavailable.	Inspected NMS dashboards to determine that managed data center physical hardware, software, and network elements were configured to be monitored for availability using the NMS.	No exceptions noted.
				Inspected NMS configurations to determine that it was configured to alert TOC staff in the event that a piece of physical hardware or element becomes unavailable.	No exceptions noted.

Additional Criteria Related to Availability and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		A1.1.3	US Signal monitors capacity within the environment on a monthly basis. Monitoring performed includes, but is not limited to, power usage, floor and cabinet space, storage capacity, and bandwidth metrics.	Inspected the capacity planning and data center huts tracking reports for a selection of months to determine that management monitored capacity within the US Signal environment on a monthly basis.	No exceptions noted.
		CC3.1.2	US Signal monitors service-level statistics on a quarterly basis to ensure that they are meeting company objectives. Results of the monitoring are communicated to management for review.	Inspected the service-level statistics for a selection of quarters to determine statistics and company objectives were monitored on a quarterly basis by US Signal.	No exceptions noted.
				Inspected the meeting invite and agenda for a selection of quarters to determine service level statistics were communicated to management for review on a quarterly basis.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2.1	Backups of the OMNI application databases are performed utilizing replication utilities. Backups are automatically monitored for errors and, if any, an alert is sent.	Inspected the configuration of the replication utilities to determine that the OMNI application databases were replicated.	No exceptions noted.

Additional Criteria Related to Availability and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
	164.308(a)(1)(ii)(B) Security Management Process: Risk Management 164.308(a)(7)(i) Contingency Plan 164.308(a)(7)(ii)(A) Contingency Plan: Data Backup Plan 164.308(a)(7)(ii)(C) Contingency Plan: Emergency Mode Operation 164.310(a)(2)(i) Facility Access Controls: Contingency Operations 164.310(d)(2)(iv) Device and Media Controls: Data Backup and Storage 164.312(a)(2)(ii) Access Controls: Emergency Access Procedure			Inspected the alert configuration and an example alert email to determine that backups were automatically monitored for errors.	No exceptions noted.
		A1.2.2	Active Directory domain data is electronically replicated on a real-time basis from the servers in Grand Rapids, Michigan to another US Signal facility.	Inspected the domain controller configurations to determine that they were configured to replicate the Active Directory domain data in real time from the servers in Grand Rapids, Michigan to another US Signal facility.	No exceptions noted.
		A1.2.3	An incremental backup of production network router configurations is performed on a daily basis.	Inspected backup schedule configurations for the production network routers and network router backup procedures to determine that backups were configured to be performed on a daily basis.	No exceptions noted.
		A1.2.4	The backup system sends a Daily Node Backup report to the Transport Engineering email distribution group indicating the number of node backups attempted and any failures that occurred.	Inspected backup system configurations and an example Daily Node Backup Report for backup failures to determine that the Transport Engineering Group received the report on a daily basis, and it indicated the number of node backups attempted and failed.	No exceptions noted.

Additional Criteria Related to Availability and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		A1.2.5	Fire and smoke detectors, automated clean-agent or pre-action wet fire suppression systems, and hand-held fire extinguishers are in place to protect US Signal data center facilities from fire-related hazards.	For each US Signal data center facility, observed the following operational system components to determine that the facility was protected from fire-related hazards: • Fire and smoke detectors • Automated clean-agent or pre-action wet fire suppression system • Handheld fire extinguishers	No exceptions noted.
		A1.2.6	The data center facilities feature dedicated climate control systems to control the temperature and humidity within the facilities.	For each US Signal data center facility, observed operational climate control systems to determine that systems were in place to control the temperature and humidity within the facility.	No exceptions noted.
		A1.2.7	UPS units and power generation equipment protect the server and telecommunication equipment from power surges and sudden power outages.	For each US Signal data center facility, observed the operational UPS units and power generation equipment to determine that systems were in place to protect corporate and telecommunication equipment from power surges and sudden power outages.	No exceptions noted.

Additional Criteria Related to Availability and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		A1.2.8	A Business Continuity and Disaster Recovery Manual has been established, and the manual is reviewed and tested at least annually.	Inspected the US Signal Business Continuity and Disaster Recovery Manual to determine that a manual had been established and was reviewed at least annually.	No exceptions noted.
				Inspected the Business Continuity and Disaster Recovery Summary document to determine that disaster recovery and business continuity tests were performed on an annual basis.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives. 164.308(a)(7)(ii)(B) Contingency Plan: Disaster Recovery Plan 164.308(a)(7)(ii)(D) Contingency Plan: Testing and Revision Procedure	A1.3.1	A restore test on backups is performed on at least an annual basis to test the recoverability of backups.	Inspected the restore test on backups to determine that it was performed on an at least annual basis.	No exceptions noted.
		A1.2.8	A Business Continuity and Disaster Recovery Manual has been established, and the manual is reviewed and tested at least annually.	Inspected the US Signal Business Continuity and Disaster Recovery Manual to determine that a manual had been established and was reviewed at least annually.	No exceptions noted.
				Inspected the Business Continuity and Disaster Recovery Summary document to determine that disaster recovery and business continuity tests were performed on an annual basis.	No exceptions noted.

Additional Criteria Related to Confidentiality and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. 164.312(c)(1) Integrity 164.316(b)(2)(i) Documentation: Time Limit 164.310(b) Workstation Use	C1.1.1	US Signal performs a quarterly data retention and destruction audit to ensure data retention and destruction procedures are being followed.	Inspected the US Signal Data Protection Policy and Record Management Policy to determine it documented US Signal's data retention and destruction procedures.	No exceptions noted.
				Inspected audit reports for a selection of quarters to determine management performed a quarterly data audit to ensure US Signal's data retention and destruction procedures were being followed.	No exceptions noted.
		C1.1.2	US Signal's office location is equipped with locked shredding containers to allow for employees to properly dispose of confidential information.	Observed US Signal's office location to determine the location was equipped with locked shredding containers to allow for employees to properly dispose of confidential information.	No exceptions noted.
		CC6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the Data Protection Policy and the Data Sanitization Policy to determine that formal data retention and disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.

Additional Criteria Related to Confidentiality and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		CC6.7.4	Storage for workstations and laptops is encrypted at rest via BitLocker.	Inspected BitLocker for a selection of workstations and laptops to determine that information in storage was encrypted at rest.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality. 164.312(c)(1) Integrity	C1.2.1	Upon customer request or the termination of a customer contract, US Signal will destroy the customer data in accordance with the Data Protection Policy.	Inspected the management console for a selection of data destruction requests from customers to determine that data was destroyed by US Signal as requested.	No exceptions noted.
		CC6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the Data Protection Policy and the Data Sanitization Policy to determine that formal data retention and disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
		CC6.5.2	Equipment potentially storing digital media is degaussed, sanitized, and/or securely destroyed prior to the equipment being removed from the US Signal facility or data centers.	Inspected the erasure log output for a selection of equipment removed from the US Signal facility or data centers to determine that equipment potentially storing digital media was degaussed, sanitized, and/or securely destroyed prior to the equipment being removed from the US Signal facility or data centers.	No exceptions noted.

Additional Criteria Related to Confidentiality and Applicable Requirements of the HIPAA Security Rule

Criteria	Trust Services Criteria and HIPAA Security Rule Reference	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		C1.1.1	US Signal performs a quarterly data retention and destruction audit to ensure data retention and destruction procedures are being followed.	Inspected the US Signal Data Protection Policy and Record Management Policy to determine it documented US Signal's data retention and destruction procedures.	No exceptions noted.
				Inspected audit reports for a selection of quarters to determine management performed a quarterly data audit to ensure US Signal's data retention and destruction procedures were being followed.	No exceptions noted.

Additional Considerations Related to the HIPAA Security Requirements Provided Within 45 CFR Sections 164.308-316

45 CFR Section Number	HIPAA Security Requirements Provided Within 45 CFR Sections 164.308-316	Control Number	Controls Specified by US Signal Company, LLC	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
H1	164.310(a)(2)(iv) Facility Access Controls: Maintenance Records	H1.1	US Signal maintains a log of repairs and modifications to the physical components of the facilities related to security.	Inspected the Data Center Preventative Maintenance Report to determine US Signal maintained a log of repairs and modifications to the physical components of the facilities related to security.	No exceptions noted.
H2	164.310(b) Workstation Use	H2.1	Employees are instructed as to the proper use of workstations, hardware, and electronic media via the Corporate Acceptable Use Policy.	Inspected the Corporate Acceptable Use Policy to determine employees were instructed as to the proper use of workstations, hardware, and electronic media via the Information Technology Acceptable Use Policy.	No exceptions noted.
H3	164.308(a)(7)(ii)(E) Contingency Plan: Applications and Data Criticality Analysis	H3.1	A BIA is performed on an annual basis to document the potential effects of an interruption to critical business operations.	Inspected the BIA report to determine a BIA was performed on an annual basis to document the potential effects of an interruption to critical business operations.	No exceptions noted.