PEAK 10, INC.

INDEPENDENT PRACTITIONER'S REPORT ON THE INFORMATION SECURITY PROGRAM FOR THE DATA CENTER OPERATIONS AND CLOUD SERVICES SYSTEM RELATED TO THE HIPAA SECURITY RULE

NOVEMBER 1, 2016, TO OCTOBER 31, 2017

Attestation and Compliance Services

Table of Contents

SECTION I

INDEPENDENT PRACTITIONER'S REPORT

INDEPENDENT PRACTITIONER'S REPORT

To Peak 10, Inc.:

Scope

We have examined Peak 10, Inc.'s ("Peak 10" or the "service organization") management's assertion that the description of its information security supporting the Data Center Operations and Cloud Services system that was provided to customer organizations (or "user entities") as of throughout the period November 1, 2016, to October 31, 2017, and included in Section 3 (the "description"), is fairly presented and that the information security program conforms, throughout the period November 1, 2016, to October 31, 2017, *to the applicable implementation specifications within the* Health Insurance Portability and Accountability Act ("HIPAA") *Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule"),* in accordance with the criteria set forth in Section 2 ("management's assertion").

Peak 10 uses BAE Systems, Inc ("BAE Systems") for Peak 10's threat detection, log file monitoring and security scanning services. The description in Section 3 includes only the information security of Peak 10 and excludes the controls, procedures, and the information security of BAE Systems. Our examination did not extend to controls, procedures, and the information security program at BAE Systems.

In Section 5, Peak 10 has provided additional information that is not a part of Peak 10's description. Information about Peak 10's management responses to exceptions noted has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to meet the HIPAA Security Rule.

Peak 10's responsibilities

Peak 10 has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria. Peak 10 is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services and related controls covered by the description; determining the *applicability of the implementation specifications; and implementing the controls described therein* for conformance of its information security program to meet the HIPAA Security Rule.

Independent practitioner's responsibilities

Our responsibility is to express an opinion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence regarding the supporting information security program supporting the Data Center Operations and Cloud Services system and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to the information security program. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the effectiveness of the information security program, is subject to the risk that controls may become inadequate or fail.

Opinion

In our opinion, based on the criteria described in Peak 10's assertion in Section 2,

a. the description fairly presents the information security program supporting the Data Center Operations and Cloud Services system that was provided to user entities, throughout the period November 1, 2016, to October 31, 2017;

b. the information security program conformed to the applicable implementation specifications within *the* HIPAA Security Rule, throughout the period November 1, 2016, to October 31, 2017; and

c. the controls specified operated effectively to provide reasonable assurance that the information security program conformed to the applicable implementation specifications within the HIPAA Security Rule, throughout the period November 1, 2016, to October 31, 2017.

Restricted use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Peak 10 and user entities of the Data Center Operations and Cloud Services system that was provided to user entities throughout the period November 1, 2016, to October 31, 2017, who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Peak 10;
- The nature of the data provided to Peak 10 and the definition of protected health information;
- How Peak 10's system interacts with user entities;
- Internal control and its limitations;
- The applicable HIPAA Security Rule; and
- The risks that may threaten the achievement of the applicable HIPAA Security Rule, 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.

Schellman & Company, LLC

Tampa, Florida
November 17, 2017

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Peak 10, Inc.'s ("Peak 10" or the "service organization") information security program supporting the Data Center Operations and Cloud Services system that was provided to customer organizations (or "user entities") throughout the period November 1, 2016, to October 31, 2017. We confirm, to the best of our knowledge, that

a. the description fairly presents the Data Center Operations and Cloud Services system made available to user entities of the system throughout the period November 1, 2016, to October 31, 2017. The criteria we used in making this assertion were that the description:

   i. presents how the information security program was designed and implemented to govern the security policies and practices supporting the Data Center Operations and Cloud Services system;

   ii. describes the relevant safeguards, standards, and rules deemed applicable by management;

   iii. describes the specified controls within the information security program designed to achieve the information security program's objectives (the "Controls");

   iv. does not omit or distort information relevant to the information security, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system, and may not, therefore, include every aspect of the Data Center Operations and Cloud Services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. The information security program supporting the Data Center Operations and Cloud Services system conforms, throughout the period November 1, 2016, to October 31, 2017, to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule"). The criteria we used in making this assertion were that:

   i. management determined the applicable Controls included in the information security program;

   ii. the Controls, as described, met implementation specifications for the applicable safeguards, standards, and rules, as defined in HIPAA Security Rule; and

   iii. the Controls, as described, were suitability designed and operated effectively throughout the period November 1, 2016, to October 31, 2017.

Section 3 of this report includes Peak 10 description of its Data Center Operations and Cloud Services system that is covered by this assertion.

SECTION 3

DESCRIPTION OF THE INFORMATION SECURITY PROGRAM

OVERVIEW OF OPERATIONS

Company Background

Peak 10, Inc. ("Peak 10") is a data center operator providing hybrid information technology (IT) infrastructure solutions spanning colocation, interconnection, cloud, managed solutions and professional services. The company combines its data centers and portfolio of hybrid IT services with localized engineering and support to serve companies nationwide. The Peak 10 management team is comprised of customer-focused professionals.

INFORMATION SECURITY PROGRAM

Description of Services Provided

Products and Services Overview

Peak 10 delivers scalable, reliable and secure IT infrastructure solutions that include data center, network, and cloud services. These services help maximize user entities' existing technology investments to better meet their current and future technology needs. From managed colocation to burstable bandwidth and cloud computing, Peak 10 IT infrastructure solutions are designed to easily scale and adapt to user entities' changing business needs.

Data Center Services

Data center services, including colocation and cloud services, are available through Peak 10's network of strategically located, secure data centers. Comprised of facilities, network, power and critical infrastructure; the Peak 10 data center services allow user entities to utilize existing investment in computing equipment and networking gear or leverage Peak 10's cloud environment.

Data Center Details

Peak 10 currently operates multiple data center facilities in 10 markets in the United States and serves companies domestically and internationally. Each of the Peak 10 data centers adheres to structured processes and procedures that ensure user entities technology assets are available and secure.

Technology and Expertise

Peak 10 facilities are staffed by a general manager and director of service delivery. The data center facilities are also manned by on-site technical experts 24/7/365 to help ensure equipment and/or critical applications are up and running, immediately accessible and secure. In addition, Peak 10 employs a comprehensive training program to help ensure that Peak 10 data center personnel are trained data center operations and security.

Technology and Security

Peak 10 data center facilities incorporate multiple physical and operational security features and protocols including the following:

- Biometric fingerprint readers
- Card/Personal Identification Number (PIN) access
- Combination lock cabinets
- 24/7/365 monitored video surveillance with video stored for review for non-repudiation.
- Multifactor authentication system
- Staff trained to maintain stringent physical security policies and controls

- Perimeter doors alarmed and monitored
- Exterior landscaping to prevent concealment of intruders

Environmental Controls/Redundancy

Designed for efficiency and cost savings, Peak 10 data centers incorporate efficient cooling solutions to ensure consistent temperature and humidity levels for protection of mission-critical technology. The data centers are also equipped with distributed cooling with cold aisle containment to help reduce energy costs. In addition, critical facility components (e.g., generators, uninterruptible power supply (UPS) and cooling systems) throughout Peak 10 data centers are redundant. With this level of redundancy, Peak 10 can perform regular preventative maintenance on the equipment with no impact to user entities.

Network

The Peak 10 network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. It incorporates redundancy to ensure reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center. Peak 10 data centers are equipped with network features, including:

- Dual path
- Redundant carrier class infrastructure
- 10/100/1000Mb ports available
- Redundant Internet access in 100Mb/1Gb/10Gb
- Multiple diverse, ring-protected fiber providers
- Multiple, redundant Tier 1 Internet access providers
- Carrier-neutral telecom services
- Metro Ethernet at 10 Mbps, 100 Mbps, 1 Gbps

Peak 10 Network Services

Peak 10 offers network services to facilitate the communication of user entity workloads running in Peak 10 data centers or the cloud with dependent systems and their users. Primary services include Internet access, Virtual Private Line (VPL) service and Ethernet Private Line (EPL) service. All options can be tailored to user entities' specific needs and are backed by 24/7/365 technical support.

Consisting of a multi-carrier, redundant architecture, the Peak 10 network has no single point-of-failure. Connectivity at each data center consists of a minimum of two fiber providers with dual entry points providing multiple gigabits of bandwidth capacity. All sites have multiple high quality Internet providers and are inter-connected via a private, meshed network. This configuration ensures network accessibility of business critical applications residing in Peak 10 data centers and/or in the Peak 10 cloud.

Peak 10 has standardized on Cisco Systems as a service provider for network architecture Cisco's ASR9000 platform provides core routing functionality in each market. The distribution layer is powered by Cisco Nexus 7000 and Catalyst 6500 series switches.

Peak 10 provides one or more local area network (LAN) connections to users' cabinets or cage space. Where redundant Peak 10 connections are needed to connect to user entities' redundant access devices, they are delivered from separate access layer switches for the final connectivity component involved in access to the Internet or other Peak 10 facilities.

Peak 10 Network Features

- Redundant paths for Internet connectivity providing connectivity to other Peak 10 locations
- Redundant carriers per location, providing flexibility to users when choosing private connectivity to their premises and trusted third parties

- Dynamic, performance optimized routing via automated, ongoing hop-count and latency monitoring Burstable services to accommodate unforeseen or seasonal demand
- Redundant, carrier-class infrastructure with no single points of failure
- 300 Gb/s aggregate intersite network capacity
- 230 Gb/s aggregate Internet capacity
- Choice of 10, 100, 1000, or 10000 Mbps access port options

Internet Access

Peak 10 Internet access solutions provide the flexibility and scalability necessary to manage expanding communications and data requirements. These services leverage industry-leading technology to optimize traffic routing to external networks to ensure availability and performance over the Internet.

In addition to bandwidth, value-add and add-on services are available for utilization monitoring, domain name service (DNS) management and IP failover services.

Features include:

- Multiple physical connectivity options including 100 Mbps, 1 Gbps and 10 Gbps network ports in addition to cloud connectivity
- Rapid installation, implementation and service change turnaround times
- Carrier neutrality for private networking needs used to connect Peak 10 housed resources to other corporate resources and third parties
- Comprehensive, web-based portal for bandwidth usage reporting
- Burstable and fixed limit subscription options
- Add-on managed security services, including firewall, virtual private network (VPN), and intrusion detection systems
- Traffic traverses Peak 10's private network without affecting Internet bandwidth usage
- Multiple 10 Gbps private connections between Peak 10 facilities

Private Network Services

User entities can use multiple Peak 10 locations to geographically diversify portions of their IT infrastructure. Connectivity between these locations is used to replicate data for a production and disaster recovery use case or to synchronize data in the case of a multi-site, active/active application deployment. Peak 10's private network provides a secure and scalable alternative to sending the data through a public Internet connection or subscribing to a private, inflexible carrier solution. Private network services can be used to carry data, video and voice services together over the same connection. Services do not traverse the public Internet and are not shared services, providing both security and reliability.

Virtual Private LAN Service

Virtual Private LAN is Peak 10's private, routed network service. It connects distinct IP subnets at each location and can provide routing to remote subnets as well for those topologies with multiple wide area network (WAN) connections. Virtual Private LAN removes the capital requirements of purchasing routing devices and the operational requirement of managing dedicated equipment.

Virtual Private LAN-specific features:

- Independent, virtual private router interfaces to provide isolated traffic flows for IP services
- Eliminate the need for user-provided routers or firewalls for IP segmentation and routing
- Lower bandwidth usage due to routed segmentation and limitation of broadcast traffic

- Scalable and available as a burstable or fixed bandwidth subscription
- Redundant access layer connectivity options are available

EPL Service

EPL provides user entities with the ability to extend local network segments, commonly referred to as a Layer 2 connectivity based on the Open Systems Interconnection (OSI) model. The service can be implemented as a scalable point-to-point or a point-to-multipoint topology. EPL is available in a wide range of bandwidth speeds and is ideal for running services and applications that require local network to be presented across geographically disparate environments within Peak 10 data centers. Additionally, user entities may choose to use this service as a component of their disaster recovery design where it is desirable not to modify local IP addresses during the failover process. EPL services also enable burstable workload scenarios where applications can be moved between locations or clouds without changes to the network configuration.

EPL-specific features:

- Independent virtual local area network (VLAN) segmentation for security
- No routing or firewall hardware required
- Utilize layer 2 switched networking to communicate across the network instead of layer 3 Transmission Control Protocol (TCP)/IP address
- Allow devices at each location to communicate as if local to each other while being on the same IP subnet
- Eliminate the use of additional routing devices to help lower latency

Data Services

Backup and Restore

Peak 10 will backup user entities' data on Peak 10 hardware, manage data backup on user entities' provided hardware, rotate tapes and manage user entities' backup library or replicate data to alternate sites.

Tape Rotation

- Peak 10 will eject media and insert next media in sequence defined by the user entities
- User entities' owned backup device and storage in the user entities' cage(s)
- Rotation scheduled by user entities

Electronic Vaulting Services

- User entity-identified data backed up to geographically remote data center
- Data sent over a secure connection
- Automated backups

Storage Services

- Enhanced tools for online management
- Security and availability
- Real-time monitoring

Availability Monitoring

- Suitable for monitoring application-specific network ports, web content and e-mail availability
- Includes up/down monitoring, TCP/User Datagram Protocol (UDP) port monitoring, Hypertext Transfer Protocol (HTTP)/ Hypertext Transfer Protocol Secure (HTTPs) content verification and e-mail round-trip monitoring

- Alerts automatically delivered via text message or e-mail to designated contact(s)

Basic Up/Down Monitoring

- Up/Down ICMP (ping) monitoring
- Suitable for any device with an IP address
- Alerts are automatically delivered via text message or e-mail to designated contact(s)

Performance Monitoring

- Suitable for most network devices which utilize the Simple Network Management Protocol (SNMP) to report performance metrics
- The subscription trends and alerts based on up/down, web and e-mail application availability, central processing unit (CPU) utilization, file system utilization, physical and virtual memory utilization, service and process status, and network interface usage, errors and discards
- Alerts are automatically delivered to the designated contact(s)

Cloud Services

The Peak 10 Cloud delivers a comprehensive computing model that allows user entities to grow their IT infrastructure as their business demands without sacrificing security, reliability or performance.

The Peak 10 Cloud enables on-demand network access to a multi-tenant environment of logically segmented pools of configurable computing resources that can be rapidly provisioned. Using the Infrastructure as a Service (IaaS) model, the Peak 10 Cloud provides on-demand resources via the Internet and/or private network connections.

The Peak 10 Cloud allows user entities to subscribe to the infrastructure and platform assets that their businesses need, while maintaining scalable, reliable and secure technology. As a result, they can operate, maintain and improve operations, enhance technology planning and manage capital/operational finances.

Enterprise Cloud

The Peak 10 Enterprise Cloud delivers compute infrastructure from scalable, enterprise-class, multi-tenant clusters. The clusters go through a commissioning process to verify that no single point of failure exists. Peak 10's Enterprise Cloud can be utilized as a standalone compute environment or can be logically connected to physical or other cloud environments.

Private Cloud

Peak 10's Private Cloud offers scale and flexibility in both virtual and dedicated service delivery models. If compliancy or user entities demands require dedicated resources or completely dedicated equipment, the Peak 10 Private Cloud can be configured to deliver the kind of platform that is needed. Peak 10 Private Cloud resource pools combine logical security and best practices with the flexibility and cost efficiency of multi-tenancy.

Recovery Cloud

The Peak 10 Recovery Cloud provides a highly flexible disaster recovery (DR) solution that ensures rapid recovery of mission-critical applications and data. Recovery Cloud enables user entities to take advantage of the reduced costs associated with multi-tenancy while accessing the necessary cloud resources to restore services in the event of a site failure quickly, securely and regardless of where their production environment is housed. It features continuous data protection (CDP) style replication to ensure data and applications are backed up in near real-time.

Description of ePHI Data Flows

Peak 10 is a data center operator that manages customers' data center, network, and cloud environments and does not create, receive, access, use, disclose, or transmit PHI and has no ability to confirm that any particular

equipment belonging to a customer contains PHI. Peak 10 customers are responsible for establishing controls to authorize, modify, evaluate/review, and revoke access to ePHI data within their environment.

Security Program Description

Peak 10 has developed an enterprise-wide information security management program to meet the information security and compliance requirements of Peak 10 and its customer base. The program was designed to help ensure the confidentiality, integrity and availability of data center operations and cloud services.

As a result, Peak 10 has adopted essential elements from the HIPAA Security Rule and implemented the necessary safeguards as specified in the Rule. The description below is a summary of security standards and safeguards Peak 10 has implemented.

The scope of the report is limited to the operations performed in the following data center facilities:

Market	Address
Atlanta	2775 Northwoods Parkway, Norcross, Georgia, 30071
	12655 Edison Drive, Alpharetta, Georgia, 30022
Charlotte	8910 Lenox Pointe Drive, Charlotte, North Carolina, 28273
	10105 David Taylor Drive, Charlotte, North Carolina, 28262
Cincinnati	5307 Muhlhauser Road, West Chester, Ohio, 45011
Jacksonville	4905 Belfort Road, Jacksonville, Florida, 32256
Louisville	752 Barret Avenue, Louisville, Kentucky, 40204
Nashville	7100 Commerce Way, Brentwood, Tennessee, 37027
	425 Duke Drive, Franklin, Tennessee, 37067
	4600 Carothers Parkway, Franklin, Tennessee, 37067
Raleigh	5150 McCrimmon Parkway, Morrisville, North Carolina, 27560
Richmond	8851-B Park Central Drive, Richmond, Virginia, 23227
South Florida	5301 NW 33rd Avenue, Fort Lauderdale, Florida, 33309
Tampa	9417 Corporate Lake Drive, Tampa, Florida, 33634
	8350 Parkedge Drive, Tampa, Florida, 33637

Administrative Safeguards

- **Security Management Process**. The organization identifies and analyzes potential risks to data center operations and cloud services, and implements security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security Personnel.** The organization designates a security official who is responsible for developing and implementing its security policies and procedures.
- **Information Access Management.** The organization implements policies and procedures for authorizing access to the data centers and cloud management environment only when such access is appropriate based on the user or recipient's role (role-based access).
- **Workforce Training and Management.** The organization provides for appropriate authorization and supervision of workforce members who work with data center operations and cloud services. The organization trains all workforce members regarding its security policies and procedures, and applies appropriate sanctions against workforce members who violate its policies and procedures.

- **Evaluation**. The organization performs a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

- **Facility Access and Control.** The organization limits physical access to its facilities while ensuring that authorized access is allowed.

Technical Safeguards

- **Access Control.** The organization implements technical policies and procedures that allow only authorized persons to access to the data centers and cloud management environment.
- **Audit Controls.** The organization implements hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use data center operations and cloud services.

Periodic Assessments

The Peak 10 risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Peak 10 executive management oversees risk management ownership and accountability. Senior management members from different operational areas are involved in the risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards and the likelihood of a threat, to determine the actions to be taken. The risk assessment process does not, however, include specific risk measurements for customer data or customer systems. Senior management also identifies significant risks based on:

- Input received from its compliance group based on their enterprise-wide risk assessment.
- Input received annually from its independent auditor based on its independent auditor's examination of the operating environment.
- Proactive monitoring of external environmental changes and other risks that relate to information security.

For any significant risk identified, management is responsible for implementing measures to monitor and manage those risks (e.g., implementing/revising control procedures, conducting specific compliance projects, etc.).

Policies and Procedures

Peak 10 has implemented policies and procedures that ensure information security is addressed throughout the organization. The policies and procedures are updated at least annually and after the periodic assessments as needed. Employees are required to sign the corporate policies acknowledgement form indicating that they have been given access to the policies and procedures as well as the privacy principles.

Subordinate Plans for Information Security

Peak 10's related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. The control activities described in Section 4 are aligned with the administrative, physical, and technical safeguards of the Security Rule.

Security Awareness Training

A security awareness training program is established that includes the following components:

- New employees are required to complete security awareness training during the on-boarding process.
- Employees are required to complete security awareness training on an annual basis.

Periodic Testing and Evaluation

Peak 10 completes third party evaluations throughout each calendar year regarding the effectiveness of the information security program that include, but are not limited to, the following:

- Independent service auditor assessments and examinations including Service Organization Control (SOC) 1 and Service Organization Control (SOC) 2 Examinations.
- Annual PCI DSS validation.
- Customer assessment based on their compliance with Sarbanes Oxley (SOX), Gramm-Leach-Bliley (GLBA), Securities and Exchange Commission (SEC) 17, Food and Drug Administration 21 CFR Part 11, the Federal Information Security Management Act (FISMA), International Traffic in Arms Regulations (ITAR), and other regulations and industry standards.
- Internal risk assessments.

Remediation and Continuous Improvement

Deficiencies in Peak 10's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person.

This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Incident Response

Peak 10 has implemented an incident response policy that is provided to all via the corporate intranet. Incident response procedures are established and distributed to specific operations personnel in charge of carrying out the procedures. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. Local and centralized technical assistance centers (TACs) are staffed 24 hours per day to respond to incidents and events. A ticketing system is utilized to document and track resolution of incidents noted.

Third Party Services and Monitoring

Peak 10 monitors the managed security services provided by BAE Systems as a component of normal business operations. Certain events identified by BAE Systems may trigger alerts / notifications to Peak 10 that require review and follow-up as applicable. Additionally, Peak 10 receives and reviews BAE Systems PCI-DSS Report on Compliance (ROC) and SOC 2 reports.

Breach Notification Description

Peak 10 has implemented a breach notification process to inform customers of breach events. Breach notification procedures are established to specific operations personnel in charge of carrying out the procedures. Following the identification of the breach, the customer will be informed notified via e-mail communications or phone call of the event. Customer communications will be sent within 30 minutes of identification and updates are sent every 60 minutes during response, escalation, and remediation. A final communication is sent to the customer notifying them of the resolution.

Risk Assessment

Risk Assessment Scoping

Peak 10 has deployed a completely independent environment for its HIPAA-Compliant services and separated the services and systems within that environment from the customer environment. Peak 10 does not create, receive, access, use, disclose, or transmit PHI and has no ability to confirm that any particular equipment belonging to a customer contains PHI. For that reason, Peak 10 does not conduct a separate risk analysis relating to locations that may house PHI.

Potential Threats, Vulnerabilities and Current Security Measures

Threat Identification

All disaster situations are ultimately managed through planning (crisis management, recovery, and continuity). Most identified risks also have been mitigated through prevention, minimization or hastened recovery resources and planning. Risks to Peak 10's data centers have been grouped into the following categories:

- Environmental
- Deliberate
- Loss of Service
- Equipment Failure
- Information Security
- Local Hazard

Vulnerability Identification

Peak 10 tracks both technical and non-technical threats and vulnerabilities in a ticketing system dedicated to security with very strict access control. When evaluating vulnerabilities, management engages the relevant internal resources and obtains available exploits via the Internet.

Peak 10 utilizes an internal vulnerability scanning tool to assess the risks posed by vulnerabilities identified. Further, a third party specialist performs an external vulnerability assessment on two externally facing environments to identify potential security vulnerabilities on a quarterly basis.

Current Security Measures

Peak 10's risk assessment methodology follows a 5-level Impact and a 5-level Probability matrix to identify the risk level of vulnerabilities, which fits right into the Common Vulnerability Scoring System (CVSS) methodology for integrating the environmental aspect of theoretical vulnerabilities.

Likelihood / Impact Analysis

Peak 10's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process usually includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed — that is, assessments of what actions need to be taken

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

Risk Level Determination / Documentation

For each identified risk, a value is assigned to the likelihood of the event on operations. Further, a value is similarly assigned of the consequences or impact potential of the risk should it manifest. These two values are added to produce a score for each given risk. Risks are documented within a risk matrix and are labeled with a risk score for how it affects the confidentiality, integrity, and availability of the system.

Risk Management Program Monitoring and Maintenance

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by corporate management, along with any other internal control evaluations. Internal control evaluations may be performed upon special request of the board of directors, senior management or departmental executives. In addition, management utilizes the work of external auditors in considering the effectiveness of internal control. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

APPLICABLE CRITERIA

Peak 10, in providing the Data Center Operations and Cloud Services, is considered a business associate. Peak 10 does not work under a covered entity's workforce but still would have access to ePHI, should ePHI be in the Data Center Operations and Cloud Services. Business associates, like covered entities, have the responsibility to achieve and maintain HIPAA compliance.

Peak 10 management has made the determination regarding the applicability of the established performance criteria as it pertains to the in-scope services (the "applicable criteria").

The table below provides the regulation references (section) and key activity, which relate to the established performance criteria, that Peak 10 management has asserted to be in-scope for the purposes of this attestation:

Section	Key Activity	Applicable Criteria	
		Yes	No
Security			
§164.306(a)	General Requirements	✓	
§164.306(b)	Flexibility of approach	✓	
§164.308(a)	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)(1)(ii)(C)	Security Management Process – Sanction Policy	✓	
§164.308(a)(1)(ii)(D)	Security Management Process --Information System Activity Review	✓	
§164.308(a)(2)	Assigned Security Responsibility	✓	
§164.308(a)(3)(i)	Workforce Security		✓
§164.308(a)(3)(ii)(A)	Workforce security -- Authorization and/or Supervision		✓
§164.308(a)(3)(ii)(B)	Workforce security -- Workforce Clearance Procedure		✓
§164.308(a)(3)(ii)(C)	Workforce security -- Establish Termination Procedures		✓
§164.308(a)(4)(i)	Information Access Management		✓
§164.308(a)(4)(ii)(A)	Information Access Management -- Isolating Healthcare Clearinghouse Functions		✓
§164.308(a)(4)(ii)(B)	Information Access Management -- Access Authorization		✓
§164.308(a)(4)(ii)(C)	Information Access Management -- Access Establishment and Modification		✓
§164.308(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, Training, and Tools -- Protection from Malicious Software	✓	
§164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools -- Log-in Monitoring	✓	
§164.308(a)(5)(ii)(D)	Security Awareness, Training, and Tools -- Password Management	✓	
§164.308(a)(6)(i)	Security Incident Procedures	✓	
§164.308(a)(6)(ii)	Security Incident Procedures -- Response and Reporting	✓	
§164.308(a)(7)(i)	Contingency Plan	✓	
§164.308(a)(7)(ii)(A)	Contingency Plan – Data Backup Plan	✓	

Section	Key Activity	Applicable Criteria	
		Yes	No
§164.308(a)(7)(ii)(B)	Contingency Plan –Disaster Recovery Plan	✓	
§164.308(a)(7)(ii)(C)	Contingency Plan -- Emergency Mode Operation Plan	✓	
§164.308(a)(7)(ii)(D)	Contingency Plan -- Testing and Revision Procedure	✓	
§164.308(a)(7)(ii)(E)	Applications and data criticality analysis		✓
§164.308(a)(8)	Evaluation of analysis	✓	
§164.308(b)(1)	Business Associate Contracts and Other Arrangements	✓	
§164.308(b)(2)	Assigned Security Responsibility	✓	
§164.308(b)(3)	Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement	✓	
§164.310(a)(1)	Facility Access Controls	✓	
§164.310(a)(2)(i)	Facility Access Controls -- Contingency Operations	✓	
§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(a)(2)(iv)	Facility Access Controls -- Maintain Maintenance Records	✓	
§164.310(b)	Workstation Use		✓
§164.310(c)	Workstation Security		✓
§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 Re-use	✓	
§164.310(d)(2)(iii)	Device and Media Controls -- Accountability		✓
§164.310(d)(2)(iv)	Device and Media Controls -- Data Backup and Storage Procedures		✓
§164.312(a)(1)	Access Control	✓	
§164.312(a)(2)(i)	Access Control -- Unique User Identification	✓	
§164.312(a)(2)(ii)	Access Control -- Emergency Access Procedure		✓
§164.312(a)(2)(iii)	Access Control -- Automatic Logoff	✓	
§164.312(a)(2)(iv)	Access Control -- Encryption and Decryption		✓
§164.312(b)	Audit Controls	✓	
§164.312(c)(1)	Integrity		✓
§164.312(c)(2)	Integrity -- Mechanism to Authenticate ePHI		✓
§164.312(d)	Person or Entity Authentication	✓	
§164.312(e)(1)	Transmission		✓
§164.312(e)(2)(i)	Transmission Security -- Integrity Controls		✓

Section	Key Activity	Applicable Criteria	
		Yes	No
§164.312(e)(2)(ii)	Transmission Security --Encryption		✓
164.314(a)(1)	Business Associate Contracts or Other Arrangements	✓	
164.314(a)(2)(i)(A)	Business associate contracts	✓	
164.314(a)(2)(i)(B)	Business associate contracts	✓	
164.314(a)(2)(i)(C)	Business associate contracts	✓	
164.314(a)(2)(ii)	Other Arrangements	✓	
164.314(a)(2)(iii)	Business associate contracts with subcontractors	✓	
164.314(a)(b)(1)	Requirements for Group Health Plans		✓
164.314(b)(2)(i)	Group Health Plan Implementation Specification		✓
164.314(b)(2)(ii)	Group Health Plan Implementation Specification		✓
164.314(b)(2)(iii)	Group Health Plan Implementation Specification		✓
164.314(b)(2)(iv)	Group Health Plan Implementation Specification		✓
§164.316(a)	Policies and Procedures	✓	
§164.316(b)(1)	Documentation	✓	
§164.316(b)(2)(i)	Documentation	✓	
§164.316(b)(2)(ii)	Documentation	✓	
§164.316(b)(2)(iii)	Documentation	✓	

The specific established performance criteria are detailed in the Testing Matrices of Section 4 of this report. It also provides the results related to the security criteria as selected from the applicability table above.

SECTION 4

TESTING MATRICES

HIPAA SECURITY RULE

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.306(a): Covered entities and business associates must do the following:(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.			
1.01	Documented security policies and procedures are in place to guide personnel in practices and principles related to the HIPAA Security Rule.	Inspected the policies and procedures to determine that documented security policies and procedures were in place to guide personnel in practices and principles related to the HIPAA Security Rule.	No exceptions noted.
§164.306(b): Flexibility of approach. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.			
1.02	A formal risk assessment is performed on at least an annual basis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that are identified are rated using a risk evaluation process and are formally documented to include, but are not limited to, the following factors: • Size, complexity, and capabilities • Technical infrastructure, hardware, and software security capabilities • Costs of security measures. • Probability and criticality of potential risks to ePHI	Inspected the most recently completed risk assessment to determine that a formal risk assessment was performed during the review period to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that were identified were rated using a risk evaluation process and were documented to include the following factors: • Size, complexity, and capabilities • Technical infrastructure, hardware, and software security capabilities • Costs of security measures. • Probability and criticality of potential risks to ePHI	No exceptions noted.
§164.308(a): A covered entity or business associate must in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.			
1.03	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.04	Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: • Health and safety • Access • Maintenance activities • Accountability	Inspected vendor access procedures to determine that documented security procedures were in place governing vendor access to the data centers that included the following: • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging	No exceptions noted.
1.05	Documented incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and include the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	Inspected the incident response and support procedures to determine that documented incident response and support procedures were in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and included the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	No exceptions noted.
§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.			
1.06	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	Inspected the information security management system policy and risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	No exceptions noted.
1.07	A formal risk assessment is performed on an annual basis. Risks that are identified are formally documented for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).			
1.08	The data centers are protected by the following environmental controls: • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers • Multiple air-conditioning units • Water detection devices • Multiple redundant UPS systems • Fueled electric power generators	Observed the in-scope data center locations to determine that the data centers were protected by the following environmental controls: • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers • Multiple air-conditioning units • Water detection devices • Multiple redundant UPS systems • Fueled electric power generators	No exceptions noted.
1.09	Management obtains inspection reports to help ensure third party specialists inspect the fire detection and suppression systems on an annual basis.	Inspected the most recent annual third party fire detection and suppression systems inspection reports to determine that third party specialists inspected the fire detection and suppression systems during the review period.	No exceptions noted.
1.10	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	Inspected the information security management system policy and risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	No exceptions noted.
1.11	A formal risk assessment is performed on an annual basis. Risks that are identified are formally documented for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
1.12	Policies and procedures require that employees sign an acknowledgment form, upon hire and upon revision of the employee manual, indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.	Inspected the new employee hiring policies and procedures to determine that policies and procedures were in place that required employees to sign an acknowledgment form, upon hire and upon revision of the employee manual, indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the employee manual, the employee manual revision history and the employee manual acknowledgment transcripts for a sample of current employees and employees hired during the review period to determine that each sample employee signed an acknowledgement upon hire and upon revision of the employee manual, indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
1.13	Newly hired employees sign a written acknowledgment form documenting their receipt of the employee manual and understanding of the requirement to adhering to the code of conduct outlined within the manual.	Inspected the employee manual, the employee manual revision history and the employee manual acknowledgment transcripts for a sample of employees hired during the review period to determine that each sample employee signed an acknowledgement upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
1.14	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the technical writer and documentation manager regarding security training to determine that employees were required to complete security training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the training documentation for a sample of current employees and employees hired during the review period to determine that each employee sampled completed security awareness training during the review period.	No exceptions noted.
§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.			
1.15	A documented violation sanction policy is in place to guide compliance personnel in applying sanctions to employees who fail to comply with security policies.	Inspected the healthcare information privacy and security violation sanction policy to determine that a documented violation sanction policy was in place to guide compliance personnel in applying sanctions to employees who failed to comply with security policies.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.16	Policies and procedures require that employees sign an acknowledgment form, upon hire and upon revision of the employee manual, indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.	Inspected the new employee hiring policies and procedures to determine that policies and procedures were in place that required employees to sign an acknowledgment form, upon hire and upon revision of the employee manual, indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
1.17	Newly hired employees sign a written acknowledgment form documenting their receipt of the employee manual and understanding of the requirement to adhere to the code of conduct outlined within the manual.	Inspected the employee manual, the employee manual revision history and the employee manual acknowledgment transcripts for a sample of employees hired during the review period to determine that each sample employee signed an acknowledgement upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual.	No exceptions noted.
§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.			
1.18	Cloud systems are configured to log access attempts and events and send the logs to a centralized log server, which is monitored by a third party.	Inquired of the manager of network engineering regarding network device logging to determine that systems were configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
		Inspected the audit configurations for a sample of cloud systems and example logs generated during the review period to determine that each sampled cloud system was configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
1.19	An automated issue management system is utilized to document, prioritize, escalate and resolve problems affecting services provided.	Inspected the automated issue management system configurations and an example customer ticket generated during the review period to determine that an automated issue management system was utilized to document, prioritize, escalate and resolve problems affecting services provided.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.			
1.20	Documented position descriptions identify and communicate the responsibility and accountability for the information security policies.	Inspected the position descriptions for a sample of security employment positions to determine that documented position descriptions identified and communicated the responsibility and accountability for the information security policies for each security employment position sampled.	No exceptions noted.
§164.308(a)(3)(i): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		
§164.308(a)(3)(ii)(A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.			
	Customers are responsible for establishing controls to authorize and supervise workforce members who access ePHI data.		
§164.308(a)(3)(ii)(B): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		
§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		
§164.308(a)(4)(i): Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		
§164.308(a)(4)(ii)(A): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.			
	Peak 10 is not a healthcare clearinghouse.		
§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		
§164.308(a)(4)(ii)(C): Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.			
	Customers are responsible for establishing controls to authorize, modify, evaluate / review, and revoke access to ePHI data.		

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).			
1.21	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the technical writer and documentation manager regarding security training to determine that employees were required to complete security training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the training documentation for a sample of current employees and employees hired during the review period to determine that each employee sampled completed security awareness training during the review period.	No exceptions noted.
§164.308(a)(5)(ii)(A): Periodic security updates.			
1.22	Users are made aware of security updates via periodic security e-mail notifications and updated security policies communicated via internal corporate sites.	Inspected the eNewsletters for a sample of months during the review period and the learning management system to determine that security updates and refresh training opportunities were provided to employees and communicated via internal corporate sites.	No exceptions noted.
		Inspected the eLearning training portal, course catalog and a sample of training course content available to employees to determine that training courses were available to new and existing employees.	No exceptions noted.
§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software.			
1.23	An antivirus policy is in place to guide network engineering personnel in configuring antivirus software on certain production servers.	Inspected the antivirus policy to determine that an antivirus policy was in place to guide network engineering personnel in configuring antivirus software on certain production servers.	No exceptions noted.
1.24	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients on a daily basis • Scan registered clients on a weekly basis	Inspected the enterprise antivirus software configurations and registered client list to determine that enterprise antivirus software was installed on production Windows servers and workstations and configured as follows: • Scan for updates to antivirus definitions and update registered clients on a daily basis • Scan registered clients on a weekly basis	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.25	Information security personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected an example security violation ticket recorded during the review period to determine that an automated ticketing system was utilized to document security violations, responses, and resolution.	No exceptions noted.
1.26	Security reviews and external vulnerability assessments are performed by a third party vendor on quarterly basis. Remediation plans are proposed and monitored through resolution by the compliance department.	Inspected the security review documentation and external vulnerability scan reports performed for a sample of quarters during the review period to determine that security reviews and vulnerability assessments were performed by a third party vendor on a quarterly basis and that remediation plans were proposed and monitored through resolution by the compliance department.	No exceptions noted.
1.27	IT personnel perform internal vulnerability scans on in-scope systems on a quarterly basis and assess the risks posed by security vulnerabilities identified.	Inquired of the director of cloud infrastructure and the manager of network engineering to determine that IT personnel performed internal vulnerability scans on in-scope systems on a quarterly basis and assessed the risks posed by security vulnerabilities identified.	No exceptions noted.
		Inspected the internal vulnerability scans for a sample of quarters during the review period to determine that for each quarter sampled, IT personnel performed internal vulnerability scans on in-scope systems (including the network domain, badge and biometric systems, managed services backup system, firewalls, routers and switches, and the virtual hypervisor) and assessed the risks posed by security vulnerabilities identified.	No exceptions noted.
1.28	Security monitoring applications are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the monitoring applications configurations to determine that security monitoring applications were utilized to monitor and analyze the in-scope systems (including the network domain, badge and biometric systems, managed services backup system, firewalls, routers and switches, and the virtual hypervisor) for possible or actual security breaches.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.308(a)(5)(ii)(C): Procedures for monitoring log-in attempts and reporting discrepancies.			
1.29	Cloud systems are configured to log access attempts and events and send the logs to a centralized log server, which is monitored by a third party.	Inquired of the manager of network engineering regarding network device logging to determine that systems were configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
		Inspected the audit configurations for a sample of cloud systems and example logs generated during the review period to determine that each sampled cloud system was configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
1.30	Documented incident response procedures including the process for informing the entity about breaches of the system security and for submitting complaints are communicated to employees and authorized users.	Inspected the incident response and support procedures to determine that documented incident response and support procedures including the process for informing the entity about breaches of the system security and for submitting complaints were communicated to employees and authorized users.	No exceptions noted.
1.31	Information security personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected an example security violation ticket recorded during the review period to determine that an automated ticketing system was utilized to document security violations, responses, and resolution.	No exceptions noted.
§164.308(a)(5)(ii)(D): Procedures for creating, changing, and safeguarding passwords.			
1.32	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.	Inspected the network infrastructure logical security policy to determine that policies were in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.	No exceptions noted.
1.33	Network devices, virtual hypervisor and VMware hosts are configured to enforce the following user account and password controls via local account policies inherited from Active Directory: • Password minimum length • Password expiration • Password complexity requirements • Password minimum history • Invalid password account lockout threshold	Inspected the network domain password configurations to determine that network user accounts and passwords were configured to meet the following password requirements: • Minimum password length • Password expiration intervals • Invalid password account lockout threshold • Password history • Password complexity requirements	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the hypervisor authentication requirements to determine that access to VMWare hosts required two factor authentication (network domain credentials and a token).	No exceptions noted.
		Inspected the LDAP configurations to determine that the configured network devices were authenticated via LDAP which utilized the network domain default domain password and account lockout policies.	No exceptions noted.
§164.308(a)(6)(i): Implement policies and procedures to address security incidents.			
1.34	Documented incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and include the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	Inspected the incident response and support procedures to determine that documented incident response and support procedures were in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and included the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	No exceptions noted.
1.35	Information security personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected an example security violation ticket recorded during the review period to determine that an automated ticketing system was utilized to document security violations, responses, and resolution.	No exceptions noted.
§164.308(a)(6)(ii): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.			
1.36	Documented incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and include the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	Inspected the incident response and support procedures to determine that documented incident response and support procedures were in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and included the following: • Severity level definitions • Escalation procedures • Response time requirements for service alerts	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.37	Information security personnel utilize an automated ticketing system to document security violations, responses, and resolution.	Inspected an example security violation ticket recorded during the review period to determine that an automated ticketing system was utilized to document security violations, responses, and resolution.	No exceptions noted.
§164.308(a)(7)(i): Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.			
1.38	The data centers are equipped with the following environmental control systems: • Fire detection and suppression systems, including audible and visual fire alarms, pre-action dry-pipe water sprinklers and/or agent-based fire suppression systems, fire and smoke detectors, and hand-held fire extinguishers • Multiple air conditioning units to regulate temperature and humidity • Water detection devices to detect and mitigate water damage in the event of a flood or water leak • Multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage • Fueled electric power generators to provide backup power in the event of a power outage	Observed the in-scope data center locations to determine that the data centers were equipped with the following environmental control systems: • Fire detection and suppression systems, including audible and visual fire alarms, pre-action dry-pipe water sprinklers and/or agent-based fire suppression systems, fire and smoke detectors, and hand-held fire extinguishers • Multiple air conditioning units to regulate temperature and humidity • Water detection devices to detect and mitigate water damage in the event of a flood or water leak • Multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage • Fueled electric power generators to provide backup power in the event of a power outage	No exceptions noted.
1.39	Management obtains inspection reports to help ensure third party specialists inspect the following equipment according to a predefined schedule: • Fire detection and suppression systems inspected annually • Air conditioning units inspected quarterly • UPS systems inspected quarterly • Generators inspected quarterly • Generators load tested annually	Inspected the most recent annual third party fire detection and suppression systems inspection reports to determine that third party specialists inspected the fire detection and suppression systems during the review period.	No exceptions noted.
		Inspected the third party air conditioning unit inspections for a sample of quarters during the review period to determine that third party specialists inspected the air conditioning units for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the third party UPS system inspection reports for a sample of quarters during the review period to determine that third party specialists inspected the UPS systems for each quarter sampled.	No exceptions noted.
		Inspected the third party generator inspection reports for a sample of quarters during the review period to determine that third party specialists inspected the generators for each quarter sampled.	No exceptions noted.
		Inspected load test results for a sample of quarters during the review period to determine that the generators were load tested for each quarter sampled.	No exceptions noted.
1.40	Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following: • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability	Observed the use of the environmental monitoring application at each data center to determine that environmental monitoring applications were utilized to monitor the environmental systems and conditions within the data centers including the following: • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability	No exceptions noted.
		Inspected the environmental monitoring application configurations to determine that environmental monitoring applications were in place to monitor the environmental systems and conditions within the data centers including the following: • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability	No exceptions noted.
1.41	The environmental monitoring application is configured to notify operations personnel via on-screen and/or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems.	Inspected the threshold configurations and example on-screen alert notifications generated during the review period to determine that the environmental monitoring application was configured to notify operations personnel via on-screen and/or e-mail alert notifications if certain predefined thresholds were exceeded on monitored systems.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.42	For subscribing customers, disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
1.43	Disaster recovery plans are tested on at least an annual basis.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were tested on at least an annual basis.	No exceptions noted.
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
§164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.			
1.44	For subscribing customers, an automated backup system is utilized to perform scheduled system backups.	Inspected the backup system schedule and an example backup log generated during the review period for a sample of subscribed customers to determine that an automated backup system was utilized to perform scheduled system backups for each subscribed customer sampled.	No exceptions noted.
1.45	The automated backup system is configured to perform daily incremental and weekly full backups of managed services infrastructure.	Inspected the backup configurations for a sample of managed services infrastructure components to determine that the automated backup system was configured to perform daily incremental and weekly full backups for each system component sampled.	No exceptions noted.
1.46	Backup system status notifications are available for subscribing customers through the web portal.	Inspected the web portal backup status log for a sample of subscribed customers to determine that backup system status notifications were available through the web portal for each subscribed customer sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.47	IT personnel perform restoration of backup files as a component of business operations for customers subscribing to backup services.	Inquired of the vice president of governance, risk, and compliance regarding backup restorations to determine that IT personnel performed restorations of backup files as a component of business operations for customers subscribing to backup services.	No exceptions noted.
		Inspected the documentation from an example backup restore performed during the review period to determine that restores were performed as a component of business operations for customers subscribing to backup services.	No exceptions noted.
	Additional backup and recovery strategies for ePHI data are the responsibility of the customer.		
§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.			
1.48	IT personnel perform restoration of backup files as a component of business operations for customers subscribing to backup services.	Inquired of the vice president of governance, risk, and compliance regarding backup restorations to determine that IT personnel performed restorations of backup files as a component of business operations for customers subscribing to backup services.	No exceptions noted.
		Inspected the documentation from an example backup restore performed during the review period to determine that restores were performed as a component of business operations for customers subscribing to backup services.	No exceptions noted.
	Additional backup and recovery strategies for ePHI data are the responsibility of the customer.		
§164.308(a)(7)(ii)(C): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.			
1.49	For subscribing customers, disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
1.50	Disaster recovery plans are tested on at least an annual basis.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were tested on at least an annual basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	Additional business continuity plans for continuation of business operations relevant to the protection of the security of ePHI while operating in emergency mode are the responsibility of the customer.		
§164.308(a)(7)(ii)(D): Implement procedures for periodic testing and revision of contingency plans.			
1.51	For subscribing customers, disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
1.52	Disaster recovery plans are tested on at least an annual basis.	Inquired of the vice president of governance, risk, and compliance regarding disaster recovery testing to determine that disaster recovery plans were tested on at least an annual basis.	No exceptions noted.
		Inspected the disaster recovery plan documentation to determine that for subscribing customers, disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	Additional procedures for the periodic testing and revision of business continuity and contingency plans relevant to operations supporting the protection or security of ePHI are the responsibility of the customer.		
§164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.			
	Customers are responsible for the assessment of the criticality of applications and data relevant to ePHI.		
§164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.			
1.53	Security policies are reviewed and revised on an annual basis by IT management. Evidence of review is documented within the policy revision history.	Inspected the document control and management procedures policy to determine that Security policies were reviewed and revised on an annual basis by IT management and evidence of review was required to be documented within the policy revision history.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of policies and procedures to determine that the policies and procedures sampled were reviewed during the review period and evidence of review and any applicable updates made was documented within the policy revision history.	No exceptions noted.
1.54	A formal risk assessment is performed on an annual basis. Risks that are identified are formally documented for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
1.55	Security monitoring applications are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the monitoring applications configurations to determine that security monitoring applications were utilized to monitor and analyze the in-scope systems (including the network domain, badge and biometric systems, managed services backup system, firewalls, routers and switches, and the virtual hypervisor) for possible or actual security breaches.	No exceptions noted.
1.56	Security reviews and external vulnerability assessments are performed by a third party vendor on quarterly basis. Remediation plans are proposed and monitored through resolution by the compliance department.	Inspected the security review documentation and external vulnerability scan reports performed for a sample of quarters during the review period to determine that security reviews and vulnerability assessments were performed by a third party vendor on a quarterly basis and that remediation plans were proposed and monitored through resolution by the compliance department.	No exceptions noted.
§164.308(b)(1): A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. §164.308(b)(2): A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.			
1.57	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.308(b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).			
1.58	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.310(a)(1): Implement policies and procedures to limit physical access to [an entity's] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.			
1.59	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.
1.60	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN • Access card and biometric scan	Observed the use of two separate two-factor authentication systems to the data centers to determine that two separate two-factor authentication systems were utilized to control access to the data centers and that the systems required the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrances	No exceptions noted.
1.61	Visitors are required to sign-in with onsite security personnel prior to entering the data centers.	Observed the visitor registration process to determine that visitors were required to sign-in with onsite security personnel prior to entering the data centers.	No exceptions noted.
		Inspected the visitor registration log for a sample of months during the review period to determine that visitor logs were utilized throughout the review period.	No exceptions noted.
1.62	Badge access privileges of terminated employees are revoked as a component of the employee termination process.	Inspected the badge access listing for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
1.63	Data center visitors are required to be accompanied and supervised by an employee of the service organization or an authorized client escort.	Observed visitor access practices to determine that visitors were escorted through the data centers by an authorized Peak 10 employee or client escort.	No exceptions noted.
		Inspected the visitor access policies to determine that data center visitors were required to be accompanied and supervised by an authorized Peak 10 employee or client escort.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.64	Security guards are in place to monitor the facility and data center during non-business hours.	Inquired of the compliance and security analyst regarding TAC personnel staffing to determine that TAC personnel were staffed at the data center facilities 24x7 to monitor facility access and log visitors.	No exceptions noted.
		Inspected the support personnel (TAC) staffing schedule for in-scope data centers and a sample months during the review period to determine that support personnel were scheduled 24x7 for each location and month sampled.	No exceptions noted.
		Observed the in-scope data center locations to determine that security guards / personnel were onsite to monitor the facilities and data centers.	No exceptions noted.
§164.310(a)(2)(i): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.			
1.65	Customer support personnel are scheduled to be available to assist customers with issues affecting their environment 24 hours per day.	Inquired of the vice president of governance, risk and compliance regarding support personnel staffing to determine that network operations personnel were scheduled for monitoring and resolution of problems affecting services 24 hours per day.	No exceptions noted.
		Inspected the network operations personnel staffing schedule for a sample of months during the review period to determine that network operations personnel were scheduled to be staffed 24 hours per day for each month sampled.	No exceptions noted.
§164.310(a)(2)(ii): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.			
1.66	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.
1.67	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN • Access card and biometric scan	Observed the use of two separate two-factor authentication systems to the data centers to determine that two separate two-factor authentication systems were utilized to control access to the data centers and that the systems required the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrances	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.68	Visitors are required to sign-in with onsite security personnel prior to entering the data centers.	Observed the visitor registration process to determine that visitors were required to sign-in with onsite security personnel prior to entering the data centers.	No exceptions noted.
		Inspected the visitor registration log for a sample of months during the review period to determine that visitor logs were utilized throughout the review period.	No exceptions noted.
1.69	Data center visitors are required to be accompanied and supervised by an employee of the service organization or an authorized client escort.	Observed visitor access practices to determine that visitors were escorted through the data centers by an authorized Peak 10 employee or client escort.	No exceptions noted.
		Inspected the visitor access policies to determine that data center visitors were required to be accompanied and supervised by an authorized Peak 10 employee or client escort.	No exceptions noted.
§164.310(a)(2)(iii): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.			
1.70	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.
1.71	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN • Access card and biometric scan	Observed the use of two separate two-factor authentication systems to the data centers to determine that two separate two-factor authentication systems were utilized to control access to the data centers and that the systems required the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrances	No exceptions noted.
1.72	Visitors are required to sign-in with onsite security personnel prior to entering the data centers.	Observed the visitor registration process to determine that visitors were required to sign-in with onsite security personnel prior to entering the data centers.	No exceptions noted.
		Inspected the visitor registration log for a sample of months during the review period to determine that visitor logs were utilized throughout the review period.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.73	Administrator privileges to the badge access system (the ability to add, modify, or delete badge access privileges) are restricted to user accounts accessible by authorized TAC and FOE personnel.	The test of the control activity, performed in September 2017, disclosed that nine of 179 badge access system user accounts held administrator privileges that were not required based on the employees' role or status. Subsequent testing of the control activity, performed in October 2017, disclosed that administrator badge access privileges were revoked for the aforementioned user accounts.	The test of the control activity, performed in September 2017, disclosed that nine of 179 badge access system user accounts held administrator privileges that were not required based on the employees' role or status. Subsequent testing of the control activity, performed in October 2017, disclosed that administrator badge access privileges were revoked for the aforementioned user accounts.
1.74	Data center visitors are required to be accompanied and supervised by an employee of the service organization or an authorized client escort.	Observed visitor access practices to determine that visitors were escorted through the data centers by an authorized Peak 10 employee or client escort.	No exceptions noted.
		Inspected the visitor access policies to determine that data center visitors were required to be accompanied and supervised by an authorized Peak 10 employee or client escort.	No exceptions noted.
1.75	Visitors are required to wear a visitor badge while visiting the data centers.	Observed the visitor registration process to determine that visitors were required to wear a visitor badge while visiting the data centers.	No exceptions noted.
1.76	The compliance and security analyst reviews badge access of terminated employees on a monthly basis.	Inspected the security and performance metrics reviews for a sample of months during the review period to determine that the compliance and security analyst reviewed badge access privileges of terminated employees for each month sampled.	No exceptions noted.
1.77	Badge access privileges of terminated employees are revoked as a component of the employee termination process.	Inspected the badge access listing for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
§164.310(a)(2)(iv): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).			
1.78	Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: • Health and safety • Access • Maintenance activities • Accountability	Inspected vendor access procedures to determine that documented security procedures were in place governing vendor access to the data centers that included the following: • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.79	Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.	Inquired of the regional operations director regarding vendor accountability forms to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.
		Inspected the vendor accountability form for a sample of change management requests (CMRs) and incident tickets requiring maintenance during the review period to determine that a vendor accountability form was signed for each CMR sampled.	No exceptions noted.
§164.310(b): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.			
	Customers are responsible for workstations containing or accessing ePHI.		
§164.310(c): Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.			
	Customers are responsible for workstations containing or accessing ePHI.		
§164.310(d)(1): Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.			
1.80	A fixed assets control and inventory policy is in place to guide personnel in place to prevent assets from being taken off-site without prior authorization.	Inspected the fixed assets control and inventory policy to determine that a fixed assets control and inventory policy was in place to guide personnel in place to prevent assets from being taken off-site without prior authorization.	No exceptions noted.
§164.310(d)(2)(i): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.			
1.81	A media disposal policy is in place to guide personnel in the disposal of backup and removable media.	Inspected the infrastructure media disposal policy to determine that a media disposal policy was in place to guide personnel in the disposal of backup and removable media.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.310(d)(2)(ii): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.			
1.82	A media disposal policy is in place to guide personnel in the removal of data from electronic media before the media are made available for re-use.	Inquired of the vice president of governance risk and compliance regarding media disposal and re-use to determine that procedures for removing PHI from media before re-use included the following: • Reformat each server • Swap drives between servers after formatting • Rebuild RAID array on each server • Format and provision new storage	No exceptions noted.
		Inspected the infrastructure media disposal policy to determine that a media disposal policy was in place to guide personnel in the removal of data from electronic media before the media are made available for re-use.	No exceptions noted.
§164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.			
	Customers are responsible for notifying Peak 10 for any request to move hardware or electronic media containing ePHI.		
§164.310(d)(2)(iv): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.			
	Customers are responsible for notifying Peak 10 of any requests to backup or create a retrievable, exact copy of ePHI, when needed, prior to movement of equipment.		
§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).			
1.83	The cloud systems are configured to enforce the following user account and password controls via local account policies inherited from Active Directory: • Minimum password length • Password expiration intervals • Invalid password account lockout threshold • Password history • Password complexity requirements	Inspected the network domain password configurations to determine that network user accounts and passwords were configured to meet the following password requirements: • Minimum password length • Password expiration intervals • Invalid password account lockout threshold • Password history • Password complexity requirements	No exceptions noted.
		Inspected the hypervisor authentication requirements to determine that access to VMWare hosts required two factor authentication (network domain credentials and a token).	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the LDAP configurations to determine that the configured network devices were authenticated via LDAP which utilized the network domain default domain password and account lockout policies.	No exceptions noted.
1.84	Network administrators utilize predefined access groups to assign user access to the network.	Inspected the network user and group access privileges to determine that network administrators utilized predefined access groups to assign user access to the network.	No exceptions noted.
1.85	Administrative privileges on the managed services network are restricted to user accounts accessible by persons holding the following positions: • Vice president of network and cloud infrastructure • Director of cloud infrastructure • Network engineering manager • Senior infrastructure engineers (5) • Senior network engineer • Infrastructure engineers (2) • Advanced services engineers (2) • Network engineer	Inspected the network domain administrative privileges with the assistance of the senior infrastructure engineer to determine that administrative privileges on the managed services network were restricted to user accounts accessible by persons holding the following positions: • Vice president of network and cloud infrastructure • Director of cloud infrastructure • Network engineering manager • Senior infrastructure engineers (5) • Senior network engineer • Infrastructure engineers (2) • Advanced services engineers (2) • Network engineer	No exceptions noted.
§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.			
1.86	Cloud system users are authenticated via a user account and password before being granted access to the devices. User identity is included in the cloud system log entries.	Inspected the user account listings and minimum password requirements for a sample of in-scope systems (including the network domain, network devices (firewalls, routers and switches), and the virtual hypervisor) to determine that each sampled in-scope system was configured to enforce predefined user account and minimum password requirements.	No exceptions noted.
		Inspected the audit configurations for a sample of cloud systems and example logs generated during the review period to determine that each sampled cloud system was configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.			
	Customers are responsible for establishing procedures for obtaining necessary ePHI during an emergency.		
§164.312(a)(2)(iii): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.			
1.87	Cloud network devices are configured to terminate inactive sessions after a predefined period of inactivity.	Inspected the session timeout configurations to determine that cloud systems were configured to terminate inactive sessions after a period of inactivity.	No exceptions noted.
§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.			
	Customers are responsible for the encryption / decryption of ePHI.		
§164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.			
1.88	Cloud systems are configured to log access attempts and events and send the logs to a centralized log server, which is monitored by a third party.	Inquired of the manager of network engineering regarding network device logging to determine that systems were configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
		Inspected the audit configurations for a sample of cloud systems and example logs generated during the review period to determine that each sampled cloud system was configured to log access attempts and events and that logs were sent to a centralized log server monitored by a third party.	No exceptions noted.
§164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.			
	Customers are responsible for the protection of ePHI data from improper alteration or destruction.		
§164.312(c)(2): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.			
	Customers are responsible for the mechanisms to corroborate that ePHI data has not been altered or destroyed in an unauthorized manner.		

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.			
1.89	The cloud systems are configured to enforce the following user account and password controls via local account policies inherited from Active Directory: • Minimum password length • Password expiration intervals • Invalid password account lockout threshold • Password history • Password complexity requirements	Inspected the network domain password configurations to determine that network user accounts and passwords were configured to meet the following password requirements: • Minimum password length • Password expiration intervals • Invalid password account lockout threshold • Password history • Password complexity requirements	No exceptions noted.
		Inspected the hypervisor authentication requirements to determine that access to VMWare hosts required two factor authentication (network domain credentials and a token).	No exceptions noted.
		Inspected the LDAP configurations to determine that the configured network devices were authenticated via LDAP which utilized the network domain default domain password and account lockout policies.	No exceptions noted.
§164.312(e)(1): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.			
	Customers are responsible for the transmission of ePHI over an electronic communications network.		
§164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.			
	Customers are responsible for ensuring that electronically transmitted ePHI data is not improperly modified without detection until disposed of.		
§164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.			
	Customers are responsible for the encryption of ePHI data.		
§164.314(a)(1): The contract or other arrangement between the covered entity and its business associate required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.			
1.90	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	Inspected the PHI business associate agreement management policy to determine that a policy was in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.91	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(2)(i)(A): The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart.			
1.92	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	Inspected the PHI business associate agreement management policy to determine that a policy was in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	No exceptions noted.
1.93	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(2)(i)(B): The contract must provide that the business associate will, in accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section.			
1.94	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	Inspected the PHI business associate agreement management policy to determine that a policy was in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	No exceptions noted.
1.95	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(2)(i)(C): The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.			
1.96	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	Inspected the PHI business associate agreement management policy to determine that a policy was in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.97	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(2)(ii): The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).			
1.98	Policies and procedures are in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	Inspected the PHI business associate agreement management policy to determine that a policy was in place to guide personnel in the selection and engagement with business associates or subcontractors who create, receive, maintain, or transmit electronic protected health information.	No exceptions noted.
1.99	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(2)(iii): The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.			
1.100	A business associate agreement is in place to define responsibilities with subcontractors associated with ePHI.	Inspected the standard business associate agreement to determine that the business associate agreement was in place to define responsibilities with covered entities and subcontractors associated with PHI.	No exceptions noted.
§164.314(a)(b)(1): Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.			
	Peak 10 is not a group health plan.		
§164.314(b)(2)(i): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.			
	Peak 10 is not a group health plan.		
§164.314(b)(2)(ii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.			
	Peak 10 is not a group health plan.		
§164.314(b)(2)(iii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.			
	Peak 10 is not a group health plan.		

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.314(b)(2)(iv): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.			
	Peak 10 is not a group health plan.		
§164.316(a): Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.			
1.101	Documented security policies and procedures are in place to guide personnel in practices and principles related to the HIPAA Security Rule.	Inspected the policies and procedures to determine that documented security policies and procedures were in place to guide personnel in practices and principles related to the HIPAA Security Rule.	No exceptions noted.
§164.316(b)(1): (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment.			
1.102	Policies and procedures are in place that address the entity maintaining written policies and procedures related to the security rule and written documents of (if any) actions, activities, or assessments required of the HIPAA Security Rule.	Inspected the records management and document retention policy to determine that policies and procedures were required to be maintained and managed by the documentation manager. Additionally, inspected evidence of documents that were maintained on the internal site to determine that HIPAA policies were policies and procedures were in place that addressed the entity maintaining written policies and procedures related to the security rule.	No nonconformities noted.
§164.316(b)(2)(i): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.			
1.103	Policies and procedures are in place that address required documentation being retained for six years from the date of its creation or the date when it last was in effect.	Inspected the document control and management procedures to determine that documents were retained in the Document Management System until they were deemed inapplicable by the business area manager and the documentation manager. Additionally, determined that documents that were retired remained on the Master Document List indefinitely with a status of retired.	No exceptions noted.
1.104	Action, activity, or assessment documentation is maintained for six years from the date of its creation or the date when it last was in effect.	Inspected the document control and management policy revision history to determine that action, activity, or assessment documentation was maintained for six years from the date of its creation or the date when it last was in effect.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.316(b)(2)(ii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.			
1.105	Security policies are communicated to the user community via the corporate intranet site.	Inspected the corporate intranet site to determine that security policies were communicated to the user community via the corporate intranet site.	No exceptions noted.
§164.316(b)(2)(iii): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.			
1.106	Policies and procedures are in place that dictate the review and update of HIPAA Security Rule related policies and procedures on a predefined basis.	Inspected the document control and management procedures policy to determine that Peak 10 policies and procedures were scheduled to be reviewed based on the class assigned to the document (according to a predefined basis).	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
§164.310(a)(2)(iii): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.			
1.73	Administrator privileges to the badge access system (the ability to add, modify, or delete badge access privileges) are restricted to user accounts accessible by authorized TAC and FOE personnel.	The test of the control activity, performed in September 2017, disclosed that nine of 179 badge access system user accounts held administrator privileges that were not required based on the employees' role or status. Subsequent testing of the control activity, performed in October 2017, disclosed that administrator badge access privileges were revoked for the aforementioned user accounts.	The test of the control activity, performed in September 2017, disclosed that nine of 179 badge access system user accounts held administrator privileges that were not required based on the employees' role or status. Subsequent testing of the control activity, performed in October 2017, disclosed that administrator badge access privileges were revoked for the aforementioned user accounts.
Management's Response:	Through the course of our examination, Peak 10 management determined that a small number employees could perform their job functions with reduced access privileges. The privileges for these employees were reduced.		