Zayo Colocation, Inc.
Type 2 SSAE 16
2014

REPORT ON MANAGEMENT'S DESCRIPTION OF ZAYO COLOCATION, INC.'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 16 (SSAE 16) Type 2

Locations audited:

Dallas, TX

- **1950 N. Stemmons Fwy. #4006, Dallas, TX 75207**
- **8600 Harry Hines Blvd. #200, Dallas, TX 75235**

May 1, 2013 through April 30, 2014

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

A-lign

INDEPENDENT SERVICE AUDITOR'S REPORT
ON A DESCRIPTION OF ZAYO COLOCATION, INC.'S SYSTEM AND
THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

To Zayo Colocation, Inc.:

We have examined Zayo Colocation, Inc.'s ('zColo' or 'the Company') description of its Colocation Services system at its Dallas, Texas locations for processing user entities' transactions for the period May 1, 2013 through April 30, 2014, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of zColo's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

In Section 2 of this report, zColo has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. zColo is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description for the period May 1, 2013 through April 30, 2014.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in zColo's assertion in Section 2 of this report,

- the description fairly presents the system that was designed and implemented for the period May 1, 2013 through April 30, 2014.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively for the period May 1, 2013 through April 30, 2014 and user entities applied the complementary user entity controls contemplated in the design of zColo's controls for the period May 1, 2013 through April 30, 2014.
- the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period May 1, 2013 through April 30, 2014.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

The information in section 5 of management's description of zColo's system, "Other Information Provided by the Service Organization," that describes the HIPAA crosswalk, is presented by management of zColo to provide additional information and is not a part of zColo's description of its system made available to user entities during the period May 1, 2013 through April 30. 2014. Information about zColo's HIPAA crosswalk has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of zColo, user entities of zColo's system during some or all of the period May 1, 2013 through April 30, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN CPAs

May 16, 2014
Tampa, Florida

SECTION 2

ZAYO COLOCATION, INC.'S ASSERTION

Zayo Colocation, Inc.'s Assertion

May 16, 2014

We have prepared the description of Zayo Colocation, Inc.'s Colocation Services system for user entities of the system during some or all of the period May 1, 2013 through April 30, 2014, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Colocation Services system made available to user entities of the system during some or all of the period May 1, 2013 through April 30, 2014 for processing their transactions. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      (1) The types of services provided including, as appropriate, the classes of transactions processed.

      (2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      (3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      (4) How the system captures significant events and conditions, other than transactions.

      (5) The process used to prepare reports and other information for user entities.

      (6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

      (7) Other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii. does not omit or distort information relevant to the scope of the Colocation Services system, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Colocation Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

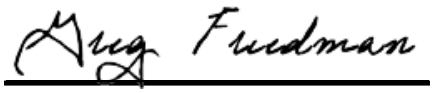
b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. The controls related to the control objectives stated in the description were suitably designed and operated effectively for the period May 1, 2013 through April 30, 2014 to achieve those control objectives. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Greg Friedman
Vice President
Zayo Colocation, Inc.

SECTION 3

DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION

OVERVIEW OF OPERATIONS

Company Background

Zayo Group is global provider of bandwidth infrastructure services, including dark fiber, wavelengths, Ethernet, lit and IP services, and carrier-neutral colocation and interconnection. Its 79,000 route mile network connects locations in and between cities on dense metro and intercity fiber assets. Zayo's network serves 297 markets in eight countries and 45 states, plus Washington, D.C. Zayo's fiber network connects the largest U.S. and European cities as well as many Tier 2-5 U.S. markets. Zayo's network reaches over 14,490 buildings, including 650 data centers, 589 carrier POPs, and 7,982 enterprise buildings. The company was founded in 2007 and is headquartered in Boulder, Colorado.

Description of Services Provided

- Dark Fiber: leveraging existing Zayo fiber assets and organic construction.
- Wavelengths: scalable WDM transport.
- Private Line: protected, dedicated connection for data, video, and voice.
- Ethernet: MEF-Certified Ethernet product portfolio.
- IP Services: IP Transit, Dedicated Internet Access (DIA), IP-VPN.
- Carrier-Neutral Colocation and Interconnection: dedicated facilities to house equipment and connect to external networks.
- Mobile Infrastructure: Small Cells and Distributed Antenna Infrastructure Systems (DAS), Tower Backhaul, and MSC Connectivity Solutions.

Zayo's bandwidth infrastructure services are used by wireless and wireline carriers, media and content companies, governments, and high-bandwidth enterprises, including healthcare, education, financial services, logistics, technology, and numerous other industries.

Information Security

zColo is primarily responsible for providing power, security, and access to the data centers. There may be additional services that are separately agreed upon with the customers. zColo will investigate and respond to fault calls or queries relating to the colocation space and to the service issues raised by the customer. As part of the Services, they provide customers with in person or on-site advice (depending on the nature of the query) or by telephone or email (as appropriate) during Business Hours, in order to assist in resolving the difficulties and queries relating to the colocation space.

zColo provides the customers with visitation procedures and, with such, other documentation and information as may be necessary for the proper use of the colocation space including updates to such documentation from time to time. Customers have access to support personnel at all times, 24/7, unless otherwise specified within their contracts.

The Colocation Service comprises:

- Racks
- Caging
- Main electrical power
- Back up electrical power
- Environmental conditioning
- Fire detection and extinguishing systems
- Access and security control systems

Racks/Cabinets

Rack space provided by zColo enables customer organizations to co-locate servers within the data center facility. The rack space provided is detailed below:

- Standard rack space expandable to meet the customer's requirements
- Air space front and back (grille doors)
- Lockable back and front doors
- Power distribution units (PDUs) each with current (amps) consumption indicators
- Main electrical power to each rack
- Cabinets
- Custom private cages

Back Up Electrical Power

Upon experiencing a main failure the backup power is provided by UPS batteries and diesel generators with automatic mains failure (AMF) start up.

UPS Battery and Diesel Generator

The details of the UPS battery and diesel generator are as follows:

- Back up batteries have autonomy of at least 10 minutes
- Diesel generator provides backup power generation
- On full load the generator can run for at least 24 hours, with refuel while running capability

Environmental Conditioning

The data center space is fully conditioned with a stabilized temperature and appropriate humidity. The conditioning systems are based upon water chillers feeding air conditioning units within the data center.

Fire Detection and Extinguishing Systems

The data center is protected against a fire incident. The systems deployed are as follows:

- Smoke and Ionization Detection – Entire data center is fitted with detection
- VESDA – Very Early Smoke Detection Alarms are fitted within the data area
- Fire suppression systems
- Handheld fire extinguishers

Access and Security Control Systems

Access control systems are deployed to thwart an intrusion. The facility contains security fencing, perimeter crash barriers, and anti-ram raid bull bars to prevent direct access to the facility. The exterior of the data centers are protected by crash barriers and security fencing. Closed Circuit TVs are deployed throughout the facilities and motion sensors record activity 24/7. Dedicated card access is installed at all entrances and exits with audible alarms at strategic exits.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of zColo's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of zColo's behavioral standards, including how they are communicated and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts.

They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel. The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere.
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- A new hire checklist is used to ensure required new hire screening procedures are performed for each new employee.

Commitment to Competence

zColo's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Skills testing are utilized during the hiring process to qualify the skills of personnel for certain positions.

Management's Philosophy and Operating Style

zColo's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate restructurings
- Expanded foreign operations

Management's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

Organizational Structure and Assignment of Authority and Responsibility

zColo's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility.

An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

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

Human Resources Policies and Practices

zColo's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New hire orientation checklist must be signed by each new employee after they attend orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT

ZColo has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user entities. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

Risks that are considered during management's risk assessment activities include the following:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology

Management's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user entities is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

zColo's control objectives and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of zColo's description of controls.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Strict peer review protocols and division of responsibilities and weekly management meetings to discuss outstanding items and issues provide for real time monitoring of operational activities. Regular conference calls with vendors and client organizations assist in the monitoring process. Senior management is extremely involved in the day-to-day operations of the company and provides for hands on monitoring. An independent financial audit and compliance audit take place to allow for monitoring of operations by outside parties.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

zColo utilizes commercially available applications to monitor the physical and environmental controls. zColo does not maintain or have logical access to client's production environments.

Communication Systems

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within zColo. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes, and job descriptions are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User organizations and subservice organizations are responsible for understanding and complying with their contractual obligations to zColo.
2. User organizations are responsible for notifying zColo of changes made to technical or administrative contact information.
3. User organizations are responsible for maintaining their own system(s) of record.
4. User organizations are responsible for ensuring the supervision, management and control of the use of zColo services by their personnel.
5. User organizations are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize zColo services.
6. User organizations are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. User organizations are responsible for ensuring the confidentiality of any user IDs and passwords used to access zColo's systems.

SECTION 4

TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-lign CPAs' examination of the controls of zColo was limited to the control objectives and related control activities specified by the management of zColo and did not encompass all aspects of zColo's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

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

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

In determining whether a SSAE 16 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the Physical Security Policy and Procedures document to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.
1.2	Each entrance and access door throughout the facility is locked and secured by a card scanning system to prevent entry from unauthorized persons.	Inquired of the Data Center Managers to determine that each entrance and access door throughout the facility was locked and secured by a card scanning system to prevent entry from unauthorized persons.	No exceptions noted.
		Inspected the access doors throughout the facility to determine that each entrance and access door throughout the facility was locked and secured by a card scanning system to prevent entry from unauthorized persons.	No exceptions noted.
1.3	Access to the data center floor is controlled by a badge access card reader.	Inquired of the Data Center Managers to determine that access to the data center floor was controlled by a badge access card reader.	No exceptions noted.
		Observed employees use their access badge to gain access to the data center to determine that access to the data center floor was controlled by a badge access card reader.	No exceptions noted.
1.4	Employees are granted access to the facility and onsite datacenter based on a documented resource request form completed.	Inquired of the Data Center Managers to determine that employees were granted access to the facility and onsite datacenter based on a documented resource request form completed.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected completed resource request forms for a sample of new hires to determine that employees were granted access to the facility and onsite datacenter based on a documented resource request form completed.	No exceptions noted.
1.5	Access through the main entrance to the facility is controlled with a mantrap.	Inquired of the Data Center Managers to determine that access through the main entrance to the facility was controlled with a mantrap.	No exceptions noted.
		Inspected the main facility entrance to determine that access through the main entrance to the facility was controlled with a mantrap.	No exceptions noted.
1.6	Employees, clients, and vendors are assigned badge access privileges to the facility and onsite data-center through the use of predefined access zones.	Inquired of the Data Center Managers to determine that employees, clients, and vendors were assigned badge access privileges to the facility and onsite data-center through the use of predefined access zones.	No exceptions noted.
		Inspected the badge access user listing and badge access zone definitions to determine that employees, clients, and vendors were assigned badge access privileges to the facility and onsite data-center through the use of predefined access zones.	No exceptions noted.
1.7	Employees are required to wear photo identification that includes the employee's name and company logo.	Inquired of the Data Center Managers to determine that employees were required to wear photo identification that included the employee's name and company logo.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the photo identification badge for a sample of employees at the data centers to determine that employees were required to wear photo identification that included the employee's name and company logo.	No exceptions noted.
1.8	The badge access system is configured to log successful and unsuccessful badge access attempts, including date, time, and badge identification information.	Inquired of the Data Center Managers to determine that the badge access system was configured to log successful and unsuccessful badge access attempts, including date, time, and badge identification information.	No exceptions noted.
		Inspected the system generated badge access logs for a sample of months to determine that the badge access system was configured to log successful and unsuccessful badge access attempts, including date, time, and badge identification information.	No exceptions noted.
1.9	Visitors entering the facility are met at the front desk, sign in to a visitor's log, and receive a non-functioning, temporary access badge.	Inquired of the Data Center Managers to determine that visitors entering the facility were met at the front desk, signed in to a visitor's log, and received a non-functioning, temporary access badge.	No exceptions noted.
		Observed the front lobby area and visitor sign-in process to determine that visitors entering the facility were met at the front desk, signed in to a visitor's log, and received a non-functioning, temporary access badge.	No exceptions noted.
1.10	A digital security camera system is in place to monitor and record activity at the facility entrances, internal access points and on the data-center floor.	Inquired of the Data Center Managers to determine that a digital security camera system was in place to monitor and record activity at the facility entrances, internal access points and on the data-center floor.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the central monitoring console and security cameras to determine that a digital security camera system was in place to monitor and record activity at the facility entrances, internal access points and on the data-center floor.	No exceptions noted.
1.11	Surveillance images captured by the digital security camera system are retained for 30 days.	Inquired of the Data Center Managers to determine that surveillance images captured by the digital security camera system were retained for 30 days.	No exceptions noted.
		Inspected archived surveillance images for a sample of days to determine that surveillance images captured by the digital security camera system were retained for 30 days.	No exceptions noted.
1.12	A termination notice is sent to IT to disable a terminated employee's logical and physical access.	Inquired of the Data Center Managers to determine that a termination notice was sent to IT to disable a terminated employee's logical and physical access.	No exceptions noted.
		Inspected the termination notice sent to IT for a sample of terminated personnel to determine that a termination notice was sent to IT to disable a terminated employee's logical and physical access.	No exceptions noted.
1.13	The data center is equipped with a fire suppression system and handheld fire extinguishers.	Inquired of the Data Center Managers to determine that the data center was equipped with a fire suppression system and handheld fire extinguishers.	No exceptions noted.
		Observed the fire suppression system and the handheld fire extinguishers to determine that the data center was equipped with a fire suppression system and handheld fire extinguishers.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.14	Third party specialists inspect and service the fire suppression system and handheld fire extinguishers.	Inquired of the Data Center Managers to determine that third party specialists inspected and serviced the fire suppression system and handheld fire extinguishers.	No exceptions noted.
		Inspected the latest fire alarm inspection report to determine that third party specialists inspected and serviced the fire suppression system and handheld fire extinguishers.	No exceptions noted.
1.15	Heating, Ventilating, and Air Conditioning (HVAC) units are in place to maintain air temperature and humidity levels within the data center.	Inquired of the Data Center Managers to determine that HVAC units were in place to maintain air temperature and humidity levels within the data center.	No exceptions noted.
		Observed the HVAC units on the data center floor to determine that HVAC units were in place to maintain air temperature and humidity levels within the data center.	No exceptions noted.
1.16	Third party specialists inspect and service the HVAC units.	Inquired of the Data Center Managers to determine that third party specialists inspected and serviced the HVAC units.	No exceptions noted.
		Inspected the latest HVAC maintenance report to determine that third party specialists inspected and serviced the HVAC units.	No exceptions noted.
1.17	The data center is connected to uninterruptible power supplies (UPS) to provide continuous power in the event of power disruption.	Inquired of the Data Center Managers to determine that the data center was connected to UPS to provide continuous power in the event of power disruption.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the UPS on the data center floor to determine that the data center was connected to UPS to provide continuous power in the event of power disruption.	No exceptions noted.
1.18	Maintenance on the UPS is performed on an annual basis by a third-party specialist.	Inquired of the Data Center Managers to determine that maintenance on the UPS was performed on an annual basis by a third-party specialist.	No exceptions noted.
		Inspected the latest UPS maintenance report to determine that maintenance on the UPS was performed on an annual basis by a third-party specialist.	No exceptions noted.
1.19	The data-center is connected to an on-site generator to provide backup power in the event of a primary power failure.	Inquired of the Data Center Managers to determine that the data-center was connected to an on-site generator to provide backup power in the event of a primary power failure.	No exceptions noted.
		Inspected the on-site generator to determine that the data-center was connected to an on-site generator to provide backup power in the event of a primary power failure.	No exceptions noted.
1.20	Regular generator load tests are performed for each generator.	Inquired of the Data Center Managers to determine that regular generator load tests were performed for each generator.	No exceptions noted.
		Inspected the latest generator load bank test report to determine that regular generator load tests were performed for each generator.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the facility and onsite datacenter are secure from unauthorized physical access and protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.21	Third party specialists perform semi-annual preventative maintenance on the backup generator.	Inquired of the Data Center Managers to determine that third party specialists performed semi-annual preventative maintenance on the backup generator.	No exceptions noted.
		Inspected the latest generator maintenance report to determine that third party specialists performed semi-annual preventative maintenance on the backup generator.	No exceptions noted.
1.22	A fuel delivery company provides generator fuel throughout the year and in the event of a long term power outage.	Inquired of the Data Center Managers to determine that a fuel delivery company provided generator fuel throughout the year and in the event of a long term power outage.	No exceptions noted.
		Inspected the most recent service report with the fuel delivery company to determine that a fuel delivery company provided generator fuel throughout the year and in the event of a long term power outage.	No exceptions noted.

CONTROL AREA 2 **CUSTOMER SERVICE DELIVERY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new customer accounts are authorized and set up accurately and completely, according to the contractual agreement and client requirements.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	For new customer implementations, a detailed Service Order Form showing the customer's requirements is provided to and signed by the customer.	Inspected the Service Order Form for a sample of new customers to determine that for new customer implementations, a detailed Service Order Form showing the customer's requirements was provided to and signed by the customer.	No exceptions noted.
2.2	A governing contract or an authorized management override is in place before a service order is executed.	Inquired of the Product Analyst regarding the governing contract to determine that a governing contract or an authorized management override was in place before a service order was executed.	No exceptions noted.
		Inspected service contracts with a sample of new customers to determine that a governing contract or an authorized management override was in place before a service order was executed.	No exceptions noted.
2.3	Service orders include defined activities/tasks appropriate to the service requested and the activities/tasks are processed to completion.	Inspected the service order tickets for a sample of new customers to determine that service orders included defined activities/tasks appropriate to the service requested and the activities/tasks were processed to completion.	No exceptions noted.
2.4	The customer designates authorized personnel for facility access via issued badge or written permission prior to an individual's arrival.	Inspected the system generated listing of customer personnel who have physical access to the data center for a sample of new customers to determine that the customer designated authorized personnel for facility access via issued badge or written permission prior to an individual's arrival.	No exceptions noted.

CONTROL AREA 2 **CUSTOMER SERVICE DELIVERY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new customer accounts are authorized and set up accurately and completely, according to the contractual agreement and client requirements.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.5	Monthly reports and invoices are generated for customers based upon the customer contract.	Inquired of the Product Analyst regarding customer invoicing to determine that monthly reports and invoices were generated for customers based upon the customer contract.	No exceptions noted.
		Inspected monthly invoices for a sample of customers to determine that monthly reports and invoices were generated for customers based upon the customer contract.	No exceptions noted.
2.6	Reports and invoices are posted to the customer portal in a timely manner based upon the customer contract.	Inquired of the Product Analyst regarding customer invoicing to determine that reports and invoices were posted to the customer portal in a timely manner based upon the customer contract.	No exceptions noted.
		Inspected a sample of customer portal dashboards to determine that reports and invoices were posted to the customer portal in a timely manner based upon the customer contract.	No exceptions noted.

CONTROL AREA 3 **CUSTOMER ISSUE RESOLUTION**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that customer issues are processed accurately, completely, and in a timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Customer issues received via phone call, email, or direct ticket request are recorded within the support team's ticketing system.	Inquired of the Product Analyst regarding customer issues to determine that customer issues received via phone call, email, or direct ticket request were recorded within the support team's ticketing system.	No exceptions noted.
		Inspected a support ticket from the ticketing system to determine that customer issues received via phone call, email, or direct ticket request were recorded within the support team's ticketing system.	No exceptions noted.
3.2	The support team's ticketing system automatically notifies management when response times exceeded defined parameters.	Inquired of the Product Analyst regarding the ticketing system to determine that the support team's ticketing system automatically notified management when response times exceeded defined parameters.	No exceptions noted.
		Inspected automatic email communications to management for a sample of delayed support tickets to determine that the support team's ticketing system automatically notified management when response times exceeded defined parameters.	No exceptions noted.
3.3	Customers are notified when their support ticket is closed and are provided an opportunity to reopen the ticket if not satisfied with the resolution.	Inquired of the Product Analyst regarding the ticketing system to determine that customers were notified when their support ticket was closed and were provided an opportunity to reopen the ticket if not satisfied with the resolution.	No exceptions noted.
		Inspected notifications to customers for a sample of closed support tickets to determine that customers were notified when their support ticket was closed and were provided an opportunity to reopen the ticket if not satisfied with the resolution.	No exceptions noted.

SECTION 5

OTHER INFORMATION
PROVIDED BY THE SERVICE ORGANIZATION

HIPAA CONTROLS CROSSWALK

This report is intended solely for use by the management of zColo, its customers, and their independent auditors. Any other use without the express written permission of zColo is prohibited.

The purpose of the following table is to describe the methods by which zColo Data Centers address the requirements of the HIPAA Security Rule as pertaining to the storing, maintaining and transmission of electronic healthcare information.
In our role as a colocation provider, zColo serves as either a Business Associate to Covered Entities or as a Sub-Contractor to Business Associates. zColo Data Centers advanced security and access protocols meet and in some cases exceed the recommended HIPAA Security guidelines. It is important to note that zColo does not have access to the Protected Health Information contained in the data servers housed in our facilities. As a result, some HIPAA Security requirements are not applicable to zColo.

All zColo personnel undergo periodic training on HIPAA Security protocols and procedures to ensure that healthcare customer data is secure, our policies and procedures are followed, and we are supporting the compliance requirements of our customers.

ADMINISTRATIVE SAFEGUARDS

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(1)(i)	Security Management Process - Implement policies and procedures to prevent, detect, contain and correct security violations. Policies and procedures should include the following:	Required	1.1	zColo has developed comprehensive physical security policies and procedures to prevent, detect, contain, and correct security violations.
164.308(a)(1)(ii)(A)	**Risk Analysis** - Ensures the company conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	Required	Minimally addressed by RISK ASSESSMENT section of report.	zColo's annual SSAE 16 audit provides a complete external environmental risk assessment of data center protocols and procedures to ensure the security of customer equipment. However, given business nature zColo's personnel do not have direct access to ePHI.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(1)(ii)(B)	**Risk Management** - Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. Factors identified in §164.306 include: • The size, complexity, capability of the covered entity; • The covered entity's technical infrastructure; • The costs of security measures; and • The probability and criticality of potential risks to ePHI	Required	Addressed by most of the controls.	zColo provides multiple levels of physical and electronic systems working 24/7. Generally covered by existing controls, but HIPAA-specific adjustments would be needed.
164.308(a)(1)(ii)(C)	Sanction Policy - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	Required	Organization Structure and Assignment of Authority and Responsibility section of the report indicates appropriate policies and procedures are probably in place.	Sanction policies are outlined for employees in the zColo employee handbook. Our workforce is required to read and acknowledge their understanding of these policies which include sanctions for non-compliance including but not limited to termination.
164.308(a)(1)(ii)(D)	Information System Activity Review - Implement procedures to regularly review records of information system activity, such as audit logs, access logs, access reports, security incident tracking reports.	Required	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI. zColo managed infrastructure components are regularly monitored to ensure high levels of system availability in accordance with service level agreements.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(2)	Assigned Security Responsibility- Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Required	Organization Structure and Assignment of Authority and Responsibility section of the report indicates appropriate responsibility assignments are probably in place.	Security Official – Recent Employee departure left space vacant. zColo is working to assign a new official.
164.308(a)(3)(i)	Workforce Security - Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Required	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI.
164.308(a)(3)(ii)(A)	Authorization and/or Supervision - Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Addressable	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI, however zColo's organization structure supports appropriate management and supervision of data center personnel and position descriptions have been developed.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure - Access of a workforce member (employee or computing device) to ePHI is appropriate.	Addressable	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI. zColo has strict access control policies on customer equipment as well as zColo owned systems.
164.308(a)(3)(ii)(C)	Termination Procedures - Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Addressable	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI. However, termination procedures have been developed and are followed to ensure that terminated employees logical and physical access to zColo systems and facilities is revoked timely. zColo customers are responsible for timely notification to remove customer personnel's physical access to zColo facilities and customer information system assets within the facility.
164.308(a)(4)(i)	**Information Access Management** - Policies and procedures are implemented that ensure authorizing access to ePHI and are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Required	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions - If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	Required	Not applicable – The organization is not responsible for this item.	zColo is not responsible for the isolation and protection of ePHI.
164.308(a)(4)(ii)(B)	Access Authorization - Policies and procedures are implemented for granting access to ePHI through access to workstation, transaction, program, process or other mechanism.	Addressable	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI. Physical access to customer equipment is strictly controlled and limited to authorized customer personnel.
164.308(a)(4)(ii)(C)	Access Establishment and Modification - Policies and Procedures are implemented that include establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process that are based upon the access authorization policies.	Addressable	Not applicable – The organization is not responsible for this item.	Procedures have been developed and are followed to grant access to zColo networks and shared infrastructure components to ensure that access is granted based on role and removed timely upon termination.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(5)(i)	Security Awareness Training - Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Required	Not specifically addressed.	zColo's existing training process could be adapted to meet HIPAA requirements. zColo personnel attend appropriate training in organizational policies and procedures, including security awareness and control requirements, as well as training in the correct use of IT facilities before access to IT services is granted.
164.308(a)(5)(ii)(A)	**Security Reminders** - Periodic security updates.	Addressable	Not addressed.	zColo personnel receive updates and reminders of critical Physical security requirements, including documented policies and procedures.
164.308(a)(5)(ii)(B)	Protection from Malicious Software - Implement procedures for guarding against, detecting, and reporting malicious software.	Addressable	Not applicable – The organization is not responsible for this item.	Antivirus software is installed on all zColo owned workstations and servers and systems and applications are patched with critical security patches in a timely manner. zColo corporate networks are logically segregated from customer networks and zColo employees and systems (workstations, servers, etc.) do not have direct access to customer systems.
164.308(a)(5)(ii)(C)	Log-in Monitoring - Implement procedures for monitoring log-in attempts and reporting discrepancies.	Addressable	Not applicable – The organization is not responsible for this item.	Monitoring of login activity for customer systems is the responsibility of the customer. zColo has access controls in place that both prevent and detect unauthorized logins for zColo owned/controlled systems.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(5)(ii)(D)	Password Management - Implement procedures for creating, changing, and safeguarding passwords.	Addressable	Not applicable – The organization is not responsible for this item.	Strong passwords are required for all shared infrastructure components enabling communication to customer systems. Default user accounts have been removed, disabled, or had their passwords changed from the default.
164.308(a)(6)(i)	Security Incident Procedures- Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Required	Partially addressed by 3.1, 3.2, and 3.3.	General incident procedures could be adapted to address security incidents.
164.308(a)(6)(ii)	Response and Reporting - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; document security incident and their outcomes.	Required	Partially addressed by 3.1, 3.2, and 3.3.	General incident procedures could be adapted to address security incidents. Procedures have been developed to identify and report on issues with security, including systems availability both internally to zColo and to customers.
164.308(a)(7)(i)	Contingency Plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Required	1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20, and 1.21.	zColo maintains written procedures for responding to and recovering from various disaster events. These plans do not negate the need for customers to build in disaster recovery capabilities into their systems.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(7)(ii)(A)	Data Backup Plan - Implement procedures to create and maintain retrievable exact copies of ePHI.	Required	Not applicable – The organization is not responsible for this item.	Customers are responsible for data backup and recovery for customer systems. zColo has developed backup and recovery procedures for zColo corporate systems.
164.308(a)(7)(ii)(B)	Disaster-Recovery Plan - Establish and implement procedures to restore any loss of data.	Required	Not applicable – The organization is not responsible for this item.	zColo maintains written procedures for responding to and recovering from various disaster events. These plans do not negate the need for customers to build in disaster recovery capabilities into their systems. With multiple data centers across the country, zColo customers can choose to implement alternate site recovery strategies and take advantage of other service offerings that enhance systems availability and recovery.
164.308(a)(7)(ii)(C)	**Emergency Mode Operation Plan** - Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	Required	Not applicable – The organization is not responsible for this item.	Plans for accessing and securing ePHI during an emergency are the responsibility of the customer. zColo has developed emergency and evacuation procedures that address health and safety as well as physical and environmental security concerns.
164.308(a)(7)(ii)(D)	**Testing and Revision Procedures** - Implement procedures for periodic testing and revision of contingency plans.	Addressable	Not applicable – The organization is not responsible for this item.	zColo has established procedures for periodic testing of systems.
164.308(a)(7)(ii)(E)	**Applications and Data Criticality Analysis** - Assess the relative criticality of specific applications and data in support of other contingency plan components.	Addressable	Not applicable – The organization is not responsible for this item.	Applications and data criticality is determined by the customer. zColo has identified and developed procedures to restore critical infrastructure components to minimize interruptions to customer systems availability.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(8)	**Evaluation** - Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirement.	Required	Partially addressed by SSAE 16 assessment.	Evaluation must be based upon HIPAA requirements. zColo undergoes annual SSAE 16 controls audits as well as periodic internal audits to evaluate internal control operation and effectiveness
164.308(b)(1)	**Business Associate Contracts and Other Arrangements** - A covered entity , in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	Required	Not applicable – The organization is not responsible for this item.	zColo is not responsible for items related to the maintenance of ePHI.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(b)(4)	**Written Contract or Other Arrangement** - Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangements with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements]	Required	Not applicable – The organization is not responsible for this item.	zColo, as a service provider (i.e. Business Associate) executes agreements related to the provision of services which include service level agreements. When appropriate, zColo executes Business Associate agreements as provided by customers. Key vendors that have potential logical access to shared communications infrastructure components are required to execute confidentiality agreements.

PHYSICAL SAFEGUARDS

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.308(a)(1)(i)	Security Management Process - Implement policies and procedures to prevent, detect, contain and correct security violations. Policies and procedures should include the following:	Required	1.1	zColo has developed comprehensive physical security policies and procedures to prevent, detect, contain, and correct security violations.
164.308(a)(1)(ii)(A)	**Risk Analysis** - Ensures the company conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	Required	Minimally addressed by RISK ASSESSMENT section of report.	zColo's annual SSAE 16 audit provides a complete external environmental risk assessment of data center protocols and procedures to ensure the security of customer equipment. However, given business nature zColo's personnel do not have direct access to ePHI.
164.310(a)(1)	Facility Access Controls - Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Required	1.1, 1.4	zColo has developed comprehensive policies and procedures to limit physical access to electronic information systems.
164.310(a)(2)(i)	Contingency Operations - Implement 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.	Addressable	1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20, and 1.21.	Customers are responsible for data backup and recovery for customer systems. zColo has developed backup and recovery procedures for zColo corporate systems.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.310(a)(2)(ii)	Facility Security Plan - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Addressable	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.9, 1.10, and 1.11	zColo has developed comprehensive physical security policies and procedures to restrict physical access to facilities and customer equipment to authorized parties.
164.310(a)(2)(iii)	Access Control and Validation Procedures - Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Addressable	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.9, 1.10, and 1.11	zColo has developed comprehensive physical security policies and procedures to restrict physical access to facilities and customer equipment to authorized parties.
164.310(a)(2)(iv)	Maintenance Records – Implement policies and procedures to document repairs and modification to the physical components of a facility which are related to security.	Addressable	Partially addressed by 1.14, 1.16, 1.19, 1.20, and 1.21	Records of maintenance to physical security components as well as preventative maintenance to environmental controls are maintained for each of zColo's data centers. Review and, if needed, expand tracking of maintenance to "the physical components of a facility which are related to security" (e.g, badge readers, generators, door locks, and cameras).

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.310(b)	Workstation Use - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surrounding of a specific workstation or class of workstation that can access electronic protected health information.	Required	Not applicable – The organization is not responsible for this item.	Customer data (including ePHI) cannot be accessed from zColo corporate workstations. Customers are responsible for protecting end-user computing devices with access to their applications and data hosted at zColo facilities.
164.310(c)	Workstation Security - Implement physical safeguards for all workstations that access ePHI, restrict access to authorized users.	Required	Not applicable – The organization is not responsible for this item.	Customer data (including ePHI) cannot be accessed from zColo corporate workstations. Customers are responsible for protecting end-user computing devices with access to their applications and data hosted at zColo facilities.
164.310(d)(1)	Device and Media Controls - 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.	Required	Not applicable – The organization is not responsible for this item.	zColo does not dispose of customer owned hardware or media. Controls over the safe transport and disposal of customer owned media are the responsibility of the customer.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.310(d)(2)(i)	Disposal - Implement policies and procedures to address final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Required	Not applicable – The organization is not responsible for this item.	zColo does not dispose of customer owned hardware or media. Controls over the safe transport and disposal of customer owned media are the responsibility of the customer.
164.310(d)(2)(ii)	Media Reuse - Implement procedures for the removal of ePHI from electronic media before the media are made available for re-use.	Required	Not applicable – The organization is not responsible for this item.	zColo does not dispose of customer owned hardware or media. Controls over the safe transport and disposal of customer owned media are the responsibility of the customer.
164.310(d)(2)(iii)	Accountability - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Addressable	Not applicable – The organization is not responsible for this item.	zColo does not move customer owned hardware or media. Controls over the safe transport and disposal of customer owned hardware / media are the responsibility of the customer.
164.310(d)(2)(iv)	Data Backup and Storage - Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Addressable	Not applicable – The organization is not responsible for this item.	Customers are responsible for the

TECHNICAL SAFEGUARDS

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.312(a)(1)	Access Control - Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 146.308 (a)(4) [Information Access Management].	Required	Not applicable – The organization is not responsible for this item.	zColo personnel do not have direct access to customer systems containing ePHI. Customers are responsible for protecting end-user computing devices with access to their applications and data hosted at zColo facilities.
164.312(a)(2)(i)	Unique User Identification - Assign a unique name and/or number for identifying and tracking user identity.	Required	Not applicable – The organization is not responsible for this item.	zColo corporate/data center networks require unique user names and passwords for access to zColo computing resources. Physical access to customer systems requires a combination of an access card as well as biometric authentication and a physical key or combination to a suite or equipment rack. Customer personnel with physical access to systems must be individually identified and registered in order to obtain access to the facility, the raised floor area, and the customer's cage or equipment rack.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.312(a)(2)(ii)	Emergency Access Procedure - Establish procedures for obtaining necessary electronic protected health information during an emergency.	Required	Not applicable – The organization is not responsible for this item.	Emergency procedures have been developed and deployed for each facility which includes securing the facility during an emergency. Emergency physical access provisions will be made on a customer by customer basis depending on the nature of the emergency to first ensure the safety and security of zColo and customer personnel and then the availability and security of customer systems and data.
164.312(a)(2)(iii)	Automatic Logoff - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Addressable	Not applicable – The organization is not responsible for this item.	zColo data center/corporate systems are configured to time-out after periods of inactivity. zColo does not control session timeouts or automatic logoff for customer communication or application sessions.
164.312(a)(2)(iv)	Encryption and Decryption - Implement procedures that specify a mechanism to encrypt and decrypt ePHI.	Addressable	Not applicable – The organization is not responsible for this item.	Encryption / Decryption mechanisms to protect data in transit or at rest are the responsibility of the customer.
164.312(b)	Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Required	Not applicable – The organization is not responsible for this item.	zColo utilizes automated and manual auditing techniques to monitor shared network circuit capacity/availability, as well as environmental controls in the data center. Customers are responsible for auditing / monitoring activity in their systems.
164.312(c)(1)	Integrity - Implement policies and procedures to protect ePHI from improper alteration or destruction.	Required	Not applicable – The organization is not responsible for this item.	Monitoring data integrity is the responsibility of the customer.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.312 (c)(2)	Mechanism to Authenticate Electronic Protected Health Information - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Addressable	Not applicable – The organization is not responsible for this item.	Monitoring data integrity is the responsibility of the customer.
164.312(d)	Person or Entity Authentication - Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Required	Not applicable – The organization is not responsible for this item.	zColo corporate/data center networks require unique user names and passwords for access to zColo computing resources. Physical access to customer systems requires a combination of an access card and/or biometric authentication and a physical key or combination to a suite or equipment rack. Customer personnel with physical access to systems must be individually identified and registered in order to obtain access to the facility, the raised floor area, and the customer's cage or equipment rack.
164.312(e) (1)	Transmission Security - Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Required	Not applicable – The organization is not responsible for this item.	Monitoring technical security is the responsibility of the customer.
164.312(e) (2)(i)	Integrity Controls - Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Addressable	Not applicable – The organization is not responsible for this item.	Monitoring data integrity is the responsibility of the customer.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.312(e)(2)(ii)	Encryption - Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Addressable	Not applicable – The organization is not responsible for this item.	Encryption of ePHI is the responsibility of the customer.

ORGANIZATIONAL REQUIREMENTS

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.314(a)(1)	Business associate contracts or other arrangements - A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful – (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	Required	Not applicable – The organization is not responsible for this item.	

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.314(a)(2)(i)	Business Associate Contracts - A business associate contract must provide that the business associate will: “Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health…; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract.”	Required	Not applicable – The organization is not responsible for this item.	
164.314(a)(2)(ii)	Other Arrangement - The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways.	Required	Not applicable – The organization is not responsible for this item.	

POLICIES AND PROCEDURES & DOCUMENTS REQUIRED

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.316(a)	Policies and Procedures - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard.	Required	Partially addressed by policies and procedures.	Recommend developing and implementing a "policy and procedures policymanual" to address development, communication, retention, review, update, and disposal of policy and procedure documents.
164.316(b)(1)	Documentation - Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Required	Partially addressed by policies and procedures.	Recommend developing and implementing a "policy and procedures policymanual" to address development, communication, retention, review, update, and disposal of policy and procedure documents.

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Related zColo SSAE 16 Control Activity/ Activities	Comments
164.316(b)(1)(i)	Time Limit - Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Required	Partially addressed by policies and procedures.	Recommend developing and implementing a “policy and procedures policymanual” to address development, communication, retention, review, update, and disposal of policy and procedure documents.
164.316(b)(1)(ii)	Availability - Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains	Required	Partially addressed by policies and procedures.	Recommend developing and implementing a “policy and procedures policymanual” to address development, communication, retention, review, update, and disposal of policy and procedure documents.
164.316(b)(1)(iii)	Updates - Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Required	Partially addressed by policies and procedures.	Recommend developing and implementing a “policy and procedures policymanual” to address development, communication, retention, review, update, and disposal of policy and procedure documents.